ISRAEL JOURNAL OF MATHEMATICS **226** (2018), 579–633
DOI: 10.1007/s11856-018-1708-y

FIRST-ORDER DECIDABILITY AND DEFINABILITY OF INTEGERS IN INFINITE ALGEBRAIC EXTENSIONS OF THE RATIONAL NUMBERS

BY

Alexandra Shlapentokh*

Department of Mathematics, East Carolina University, Greenville, NC 27858, USA
e-mail: shlapentokha@ecu.edu
URL: myweb.ecu.edu/shlapentokha

ABSTRACT

We extend results of Videla and Fukuzaki to define algebraic integers in large classes of infinite algebraic extensions of $\mathbb{Q}$ and use these definitions for some of the fields to show the first-order undecidability. We also obtain a structural sufficient condition for definability of the ring of integers over its field of fractions. In particular, we show that the following propositions hold: (1) For any rational prime q and any positive rational integer m, algebraic integers are definable in any Galois extension of $\mathbb{Q}$ where the degree of any finite subextension is not divisible by q^m. (2) Given a prime q, and an integer $m > 0$, algebraic integers are definable in a cyclotomic extension (and any of its subfields) generated by any set $\{\xi_{p^\ell} | \ell \in \mathbb{Z}_{>0}, p \neq q$ is any prime such that $q^{m+1} \not| (p-1)\}$. (3) The first-order theory of any abelian extension of $\mathbb{Q}$ with finitely many ramified rational primes is undecidable and rational integers are definable in these extensions.

We also show that under a condition on the splitting of one rational prime in an infinite algebraic extension of $\mathbb{Q}$, the existence of a finitely generated elliptic curve over the field in question is enough to have a definition of $\mathbb{Z}$ and to show that the field is undecidable.

* The research for this paper has been partially supported by NSF grants DMS-0650927 and DMS-1161456, and a grant from John Templeton Foundation. The author would also like to thank Carlos Videla for helpful comments.
Received May 24, 2016 and in revised from May 12, 2017

1. Introduction

The purpose of this paper is to consider the following problems of definability and decidability for an infinite algebraic extension K_{inf} of $\mathbb{Q}$.

Question 1.1: Is the ring of integers of K_{inf} first-order definable over K_{inf}?

Question 1.2: Is the first-order theory of K_{inf} decidable?

Questions of this type have a long history, especially as applied to number fields and in connection to generalizations of Hilbert's Tenth Problem. We will not attempt to give a full account of the work done in the subject here but will limit ourselves to pointing out some surveys as well as results specifically relevant to this paper.

Perhaps a good place to start is with the results of J. Robinson who proved in [25] and [26] that in any number field the ring of integers of the number field as well as the ring of rational integers are first-order definable in the language of rings, and therefore the first-order theory of these fields (in the language of rings) is undecidable. In the process of proving these results J. Robinson also proved that integrality at a prime of a number field is existentially definable in the language of rings over a number field. In [27] J. Robinson produced a uniform definition of $\mathbb{Z}$ over rings of integers of number fields. R. Rumely in [30] improved J. Robinson's results making a definition of valuation rings uniform across global fields. More recently, B. Poonen in [22] and J. Koenigsmann in [11] produced new results reducing the number of universal quantifiers used in definitions of $\mathbb{Z}$ over $\mathbb{Q}$, B. Poonen to two and J. Koenigsmann to one.

The desire to reduce the number of universal quantifiers is motivated to a large extent by the interest in extending Hilbert's Tenth Problem to $\mathbb{Q}$. This would be accomplished by a purely existential definition of $\mathbb{Z}$ over $\mathbb{Q}$. Unfortunately there are serious doubts as to whether such a definition exists. See [6], [21] and [33] for surveys on Hilbert's Tenth Problem and related questions of definability.

A lot of work aiming to prove the decidability of the first-order theory has centered around various infinite extensions of $\mathbb{Q}$. (See [6] for a survey of these results.) One of the more influential results was due to R. Rumely in [31], where he showed that Hilbert's Tenth Problem is decidable over the ring of all algebraic integers. This result was strengthened by L. van den Dries proving in [40] that the first-order theory of this ring was decidable. Another remarkable result is due to M. Fried, D. Haran and H. Völklein in [9], where it is shown that the first-order theory of the field of all totally real algebraic numbers is decidable. This field constitutes a boundary of sorts between the “decidable” and “undecidable”, since J. Robinson showed in [27] that the first-order theory of the ring of all totally real integers is undecidable. In the same paper, she also proved that the first-order theory of a family of totally real rings of integers is undecidable and produced a “blueprint” for such proofs over rings of integers which are not necessarily totally real.

Using some ideas of J. Robinson, an elaboration of J. Robinson’s “blueprint” by C. W. Henson (see page 199 of [40]), and R. Rumely’s method for defining integrality at a prime, C. Videla produced the first-order undecidability results for a family of infinite algebraic extensions of $\mathbb{Q}$ in [41], [42] and [43]. More specifically, C. Videla showed that the first-order theory of some totally real infinite quadratic extensions, any infinite cyclotomic extension with a single ramified prime, and some infinite cyclotomic extensions with finitely many ramified primes is undecidable. C. Videla also produced the first result concerning definability of the ring of integers over an infinite algebraic extension of $\mathbb{Q}$ by generalizing a technique of R. Rumely: he showed that if all finite subextensions are of degree equal to a product of powers of a fixed (for the field) finite set of primes, then the ring of integers is first-order definable over the field.

In a recent paper [10], K. Fukuzaki, generalizing the quadratic form technique of Julia Robinson, proved that a ring of integers is definable over an infinite Galois extension of the rationals such that every finite subextension has odd degree over the rationals and its prime ideals dividing 2 are unramified. He then used one of the results of J. Robinson to show that a large family of totally real fields contained in cyclotomics (with infinitely many ramified primes) has an undecidable first-order theory.

2. The statements of new results and overview of the proofs

The results of this paper can be divided into two categories: definability results, more specifically defining rings of integers and $\mathbb{Z}$ over infinite extensions, and undecidability results for infinite extensions. We discuss our new definability results first.

2.1. The new definability results: q-boundedness. For the purposes of our discussion we fix an algebraic closure $\tilde{\mathbb{Q}}$ of $\mathbb{Q}$ and consider a progression from $\mathbb{Q}$ to its algebraic closure, first through the finite extensions of $\mathbb{Q}$, next through its infinite extensions fairly "far" from the algebraic closure, and finally through the infinite extensions of $\mathbb{Q}$ fairly "close" to $\tilde{\mathbb{Q}}$.

As one gets closer to $\tilde{\mathbb{Q}}$, there is an expectation that the language of rings would loose more and more of its expressive power. It would be interesting to describe the mile posts signifying various stages of this loss. A definitive description of these mile posts is probably far away, but in this paper we consider a candidate for an early mile post for the loss of definability, the loss of what we called "q-boundedness" for all rational primes q. We define the notion of being "q-bounded" below following the first set of notation.

Notation 2.1: (1) Let $K_{\inf}$ be an infinite algebraic extension of a number field G.

(2) Let

$$I_G = I(G, K_{\inf}) = \{K | K \text{ is a number field such that } G \subseteq K \subset K_{\inf}\}.$$

(3) For any $M \in I_G$, let

$$I_M = I_M(G, K_{\inf}) = \{K | K \text{ is a number field such that } G \subseteq M \subseteq K \subset K_{\inf}\}.$$

(4) For any $M \in I_G$, let $J_M(G, K_{\inf})$ be an ordered by inclusion subset of I_M such that the union of all the fields in J_M is $K_{\inf}$. If $\mathfrak{p}_M$ is a prime of M, then prime factors of $\mathfrak{p}_M$ in the fields of J_M generate a tree. A path in such a tree corresponds to a prime ideal of $O_{K_{\inf}}$—the ring of integers of $K_{\inf}$. We will refer to J_M as a field path from M to $K_{\inf}$.

(5) If $M \in I_G$ and $\mathscr{S}_M$ is a set of primes of M, then let $O_{K_{\inf}, \mathscr{S}_{K_{\inf}}}$ denote the integral closure of $O_{M, \mathscr{S}_M}$ in $K_{\inf}$. We let $O_{K_{\inf}}$ denote the ring of algebraic integers of $K_{\inf}$.

(6) If M is a number field, $\mathfrak{p}_M$ is a prime of M, and $K \in I_M$, then let $\mathscr{C}_K(\mathfrak{p}_M)$ denote the set of all prime factors of $\mathfrak{p}_M$ in K. Let

$$\mathscr{C}_{\inf}(\mathfrak{p}_M) = \bigcup_{K \in I_M} \mathscr{C}_K(\mathfrak{p}_M).$$

We now describe conditions on the primes necessary for our definitions of integers. The two diagrams below correspond to the Definition 2.2 of q-unbounded and completely q-bounded primes.

A diagram for q-unbounded primes

$$\begin{tikzcd}
G \arrow[r, "\forall"] & M \arrow[r, "\exists"] & K \arrow[r] & \cdots \arrow[r] & K_{\mathrm{inf}} \\
\mathfrak{p}_G \arrow[u] \arrow[r, hook, "\forall"] & \mathfrak{p}_M \arrow[u] \arrow[r, hook, "\forall", "q|ef"'] & \mathfrak{p}_K \arrow[u] & &
\end{tikzcd}$$

A diagram for completely q-bounded primes

$$\begin{tikzcd}
G \arrow[r, "\exists"] & M \arrow[r, "\forall"] & K \arrow[r] & \cdots \arrow[r] & K_{\mathrm{inf}} \\
\mathfrak{p}_G \arrow[u] \arrow[r, hook, "\forall"] & \mathfrak{p}_M \arrow[u] \arrow[r, hook, "\forall", "\mathrm{ord}_q(ef)=0"'] & \mathfrak{p}_K \arrow[u] & &
\end{tikzcd}$$

Definition 2.2 (q-unbounded and q-bounded primes): Let q be a rational prime and let $\mathfrak{p}_G$ be a prime of G satisfying the following condition: for any $M \in I_G$ there exists $K \in I_M$ such that for any $\mathfrak{p}_M \in \mathscr{C}_M(\mathfrak{p}_G)$ and any $\mathfrak{p}_K$ in $\mathscr{C}_K(\mathfrak{p}_M)$ we have that

$$d(\mathfrak{p}_K/\mathfrak{p}_M) = e(\mathfrak{p}_K/\mathfrak{p}_M)f(\mathfrak{p}_K/\mathfrak{p}_M) \equiv 0 \mod q,$$

where as usual $e(\mathfrak{p}_K/\mathfrak{p}_M)$ is the ramification degree of $\mathfrak{p}_K$ over $\mathfrak{p}_M$, $f(\mathfrak{p}_K/\mathfrak{p}_M)$ is the relative degree of $\mathfrak{p}_K$ over $\mathfrak{p}_M$, and $d(\mathfrak{p}_K/\mathfrak{p}_M)$ is the local degree of $\mathfrak{p}_K$ over $\mathfrak{p}_M$. In this case we call $\mathfrak{p}_G$ **q-unbounded**. (See the diagram above.)

If there exists $M \in I_G$ such that for any $K \in I_M$, for any $\mathfrak{p}_M \in \mathscr{C}_M(\mathfrak{p}_G)$, and any $\mathfrak{p}_K$ in $\mathscr{C}_K(\mathfrak{p}_M)$ we have that $\mathrm{ord}_q\, d(\mathfrak{p}_K/\mathfrak{p}_M) = 0$, we call $\mathfrak{p}_G$ **completely q-bounded**. (See a diagram above.)

If $\mathfrak{p}_G$ is not q-unbounded, we call $\mathfrak{p}_G$ **q-bounded**. If every prime in $\mathscr{C}_{\mathrm{inf}}(\mathfrak{p}_G)$ is q-bounded, we call $\mathfrak{p}_G$ **hereditarily q-bounded**.

If every prime of G is hereditarily q-bounded in K_{inf}, and all factors of q are completely q-bounded, then we will call K_{inf} itself q-bounded.

Observe that if a prime is completely q-bounded, it is hereditarily q-bounded. As is shown below, we need all the primes of G to be hereditarily q-bounded, and we need q to be completely q-bounded for our definition method to work for the ring of integers. At the same time the unbounded primes can be used to define “big subrings”.

Remark 2.3: One can rephrase the definition of a q-unbounded prime as follows. A prime $\mathfrak{p}_G$ of G is unbounded if for every $n \in \mathbb{Z}_{>0}$ there exists a field $M \in I_G$ such that for any $\mathfrak{p}_M \in \mathscr{C}_M(\mathfrak{p}_G)$ we have that

$$e(\mathfrak{p}_M/\mathfrak{p}_G)f(\mathfrak{p}_M/\mathfrak{p}_G) = d(\mathfrak{p}_M/\mathfrak{p}_G) \equiv 0 \mod q^n,$$

where $d(\mathfrak{p}_M/\mathfrak{p}_G)$ as above is the local degree $[M_{\mathfrak{p}_M} : G_{\mathfrak{p}_G}]$.

Informally speaking, given an infinite algebraic extension K_{inf} of $\mathbb{Q}$ we consider what happens to the local degrees of primes over $\mathbb{Q}$ as we move through the factor tree within K_{inf}. A rational prime p is called **q-bounded** if it lies on a path through the factor tree in K_{inf} where the local degrees of its factors over $\mathbb{Q}$ are not divisible by arbitrarily high powers of q. If every descendant of p in every number field contained in K_{inf} has the same property, then we say that p is hereditarily q-bounded.

For q itself we require a stronger condition: the local degrees along all the paths of the factor tree should have uniformly bounded order at q. If this condition is satisfied, we say that q (or some other prime in question) is **completely q-bounded**. If all the primes $p \neq q$ are hereditarily q-bounded and q is completely q-bounded, we say that the field K_{inf} itself is q-bounded.

The main result of the paper connected to the notion of q-boundedness is the following theorem.

Theorem 1: *Let p, q be rational prime numbers, not necessarily distinct. Let H be a number field, and let H_{inf} be an algebraic extension of H. Let $\mathscr{S}_H$ be a finite, possibly empty, set of primes of H. Assume all primes of H not in $\mathscr{S}_H$ are hereditarily q-bounded in H_{inf}, and primes in $\mathscr{S}_H$ and factors of q are completely p-bounded in H_{inf}. In this case, the integral closure of $O_{H,\mathscr{S}_H}$ in H_{inf} is first-order definable over H_{inf}.*

This theorem will reappear below with a proof as Theorem 3.14. Rings of integers are also definable under some modifications of the q-boundedness assumptions. We give an example of a result of this type in Theorem 3.17. We also show that one can leverage the q-unbounded primes for the purposes of definability, i.e., to define rings where only q-unbounded primes can appear in the denominator. (See Theorem 3.16.)

Below we explain what new fields our results cover, but perhaps the most important aspect of our definability result is the structural one. We suspect that q-boundedness or a similar condition, e.g., a somewhat more general condition described in Theorem 3.17, is necessary for definability of the ring of integers. While non-definability examples are scarce over infinite extensions, we offer the following ones: the field of all totally real numbers, not satisfying the assumptions of Theorem 3.17, and decidable by the result of M. Fried, H. Völklein, and D. Haran ([9]), has the ring of integers not definable over the field, since it is undecidable by a result of J. Robinson ([26]). Further, the field of real algebraic numbers and the field of algebraic numbers also do not satisfy the assumptions of Theorem 3.17, and their rings of integers are not definable over the field by results of A. Tarski ([39]).

2.2. Results of C. Videla and K. Fukuzaki considered within the q-bounded framework. Proceeding chronologically, we reconsider results of C. Videla first. As mentioned above, his results concerned infinite Galois extensions of number fields, where all the finite subextensions are of degree divisible only by primes belonging to a fixed finite set of primes A. Consequently, in the fields considered by C. Videla all the primes are completely q-bounded for any $q \notin A$, and thus all these fields are certainly q-bounded.

The first natural extension of C. Videla's result, obtainable from our work, is the proposition that the integers are definable in any Galois extension where all the finite subextensions have degree not divisible by a single prime q (while results of C. Videla prohibit divisibility of the degrees by all but finitely many primes). Further, we can allow finitely many subextensions to be divisible by q. For this reason, while C. Videla could show that the ring of algebraic integers is definable in any cyclotomic extension of $\mathbb{Q}$ with finitely many ramified primes, we can show that the ring of integers is definable in a larger class of cyclotomic extensions, including extensions with infinitely many ramified primes. For example, for any rational prime q and any $m \in \mathbb{Z}_{>0}$ we can adjoin to $\mathbb{Q}$ all ℓ^n-th roots of unity for any positive integer n and for any rational prime ℓ such that q^m does not divide $\ell - 1$.

Turning our attention to K. Fukuzaki we note that all the fields he considers are 2-bounded. Further, K. Fukuzaki does not allow any ramification of dyadic ideals and no finite subextensions of even degrees, options we can allow even if we just consider 2-bounded fields. Thus, again as described above, K. Fukuzaki's results allow him to consider some totally real subfields of cyclotomics with infinitely many ramified primes but not the cyclotomics themselves.

Further, both C. Videla and K. Fukuzaki consider only Galois extensions, a restriction we do not require. Many more examples of q-bounded fields, some natural and some less so, can be found in Section 4. Among a set of natural examples not covered by earlier work are non-Galois fields that are towers of finite subextensions of degrees less than m for some positive integer m. We should also note that the family of fields we consider is closed under any finite extension, a property not shared by the fields considered by earlier researchers in the area. Finally all our definability results are proved more generally for the rings of $\mathscr{S}$-integers for an arbitrary finite $\mathscr{S}$, with empty $\mathscr{S}$ corresponding to the ring of integers of some number field K.

2.3. Overview of the construction of our definition of integers. The central part of our construction is a norm equation which has no solutions if a field element in question has "forbidden" poles. (In an effort to simplify terminology we transferred some function field terms to this number field setting.) While we are far from being the only or the first practitioners of this method which originates with J. Robinson and R. Rumely, we do employ a unique, to our knowledge, variation of it. More specifically, as explained below, we do not fix the top or the bottom field in the norm equation, but allow these fields to vary depending on the elements involved. As long as the degree of all extensions involved is bounded, such a "floating" norm equation is still (effectively) translatable into a system of polynomial equations over the given field. (See the proof of Theorem 3.14 for the description of this translation.)

To set up the norm equation, let

- q be a rational prime number,
- K be a number field containing a primitive q-th root of unity,
- $\mathfrak{p}_K$ be a prime of K not dividing q,
- $b \in K$ be such that $\operatorname{ord}_{\mathfrak{p}_K} b = -1$,
- $c \in K$ be such that c is integral at $\mathfrak{p}_K$ and is not a q-th power in the residue field of $\mathfrak{p}_K$,

and consider $bx^q + b^q$ for some $x \in K$. Note that $\operatorname{ord}_{\mathfrak{p}_K}(bx^q + b^q)$ is divisible by q if and only if $\operatorname{ord}_{\mathfrak{p}_K} x \geq 0$. Further, if x is an integer, all the poles of $bx^q + b^q$ must be poles of b and are divisible by q. Assume also that all zeros of $bx^q + b^q$ and all zeros and poles of c are of orders divisible by q and $c \equiv 1 \mod q^3$. Finally, to simplify the situation further, assume that either K has no real embeddings into $\tilde{\mathbb{Q}}$ or $q > 2$. Now consider the norm equation

$$\mathbf{N}_{K(\sqrt[q]{c})/K}(y) = bx^q + b^q. \tag{2.1}$$

Since $\mathfrak{p}_K$ does not split in this extension, if x has a pole at $\mathfrak{p}_K$, then

$$\mathrm{ord}_{\mathfrak{p}_K} bx^q + b^q \not\equiv 0 \mod q,$$

and the norm equation has no solution y in $K(\sqrt[q]{c})$. Further, if x is an integer, given our assumptions, using the Hasse Norm Principle we can show that this norm equation does have a solution. Our conditions on c ensure that the extension is unramified, and our conditions on $bx^q + b^q$ in the case x is an integer make sure that locally at every prime not splitting in the extension the element $bx^q + b^q$ is equal to a q-th power of some element of the local field times a unit. By the local class field theory, this makes $bx^q + b^q$ a norm locally at every prime.

For an arbitrary b and $c \equiv 1 \mod q^3$ in K, we will not necessarily have all zeros of $bx^q + b^q$ and all zeros and poles of c of orders divisible by q. For this reason, given $x, b, c \in K$ we consider our norm equation in a finite extension L of K and this extension L depends on x, b, c and q. We choose L so that all primes occurring as zeros of $bx^q + b^q$ or as zeros or poles of c are ramified with ramification degree divisible by q. We also take care to split $\mathfrak{p}_K$ completely in L, so that in L we still have that c is not a q-th power modulo any factor $\mathfrak{p}_L$ of $\mathfrak{p}_K$. This way, as we run through all $b, c \in K$ with $c - 1 \equiv 0 \mod q^3$, we "catch" all the primes that do not divide q and occur as poles of x. The construction of the field L and the argument concerning the properties of the primes in question in this field are in Propositions 7.9 and 7.10.

Unfortunately, we will not catch factors of q that may occur as poles in this manner, because our assumption on c forces all the factors of q to split into distinct factors in the extension. Splitting factors of q into distinct factors protects us from a situation where such primes may ramify and cause the norm equation not to have solutions even when x is an integer. Elimination of factors of q from the denominators of the divisors of the elements of the rings we define will be done separately.

The end result of this construction, described in detail in Section 7, is essentially a uniform definition of the form $\forall\forall\exists \ldots \exists$ of the ring of $\mathscr{Q}$-integers, with $\mathscr{Q}$ containing factors of q, across all number fields containing the q-th primitive roots of unity.

Putting aside for the moment the issue of defining the set of all elements c integral at q and equivalent to 1 mod q^3, and the related issue of defining integrality at factors of q in general, we now make the transition to an infinite q-bounded extension K_{inf} by noting the following. Let $K \subset K_{\text{inf}}$, let $\mathfrak{p}_K$ be a prime of K such that $\mathfrak{p}_K$ does not divide q, let $x \in K$ and let $\operatorname{ord}_{\mathfrak{p}_K} x < 0$. Since by assumption $\mathfrak{p}_K$ is q-bounded, it lies along a path in its factor tree within K_{inf}, where the order at q of local degrees eventually stabilizes. To simplify the situation once again, we can assume that it stabilizes immediately past K. So let N be another number field with $K \subset N \subset K_{\text{inf}}$. In this case for some prime $\mathfrak{p}_N$ above $\mathfrak{p}_K$ in N, we have that $\operatorname{ord}_q e(\mathfrak{p}_N/\mathfrak{p}_K) = \operatorname{ord}_q f(\mathfrak{p}_N/\mathfrak{p}_K) = 0$. Now, let $b, c \in K$ be as above and observe that c is not a q-th power in the residue field of $\mathfrak{p}_N$ while $\operatorname{ord}_{\mathfrak{p}_N}(bx^q + b^q) \not\equiv 0 \mod q$. Thus the corresponding norm equation with K replaced by N and eventually by K_{inf} in (2.1) has no solution. Of course when x is an integer and we have a solution to our norm equation in K, we also have a solution in K_{inf}.

Note that for each prime $\mathfrak{p}_K$ of K, at every higher level of the tree we need just one factor with the local degree not divisible by q to make the norm equation unsolvable when $\mathfrak{p}_K$ appears in the denominator of the divisor of x. Hence having one q-bounded path per every prime of K is enough to make sure that no prime of K not dividing q occurs as a pole of any element of K in our set.

Unfortunately, if we go to an extension of K inside K_{inf}, some primes of K will split into distinct factors and can occur independently in the denominators of the divisors of elements of extensions of K. Thus, in the extensions of K inside K_{inf} we have to block each factor separately. This is where the "hereditary" part comes in. We need to require the same condition of q-boundedness for every descendant in the factor tree of every prime of K not dividing q, insuring integrality at all factors of all K-primes not dividing q.

Before we tackle integrality at factors of q, we point out that a preliminary definition of the subring of an infinite extension containing only algebraic numbers with no poles outside the set of factors of q is in (3.10). Note that $\Phi_q(K_{\text{inf}})$ is precisely the set of all $c \in K_{\text{inf}}$ integral at q and equivalent to 1 mod q^3. Once we have a definition of integrality at factors of q, we will also be able to define $\Phi_q(K_{\text{inf}})$.

The main reason that only one q-bounded path per prime not dividing q is enough to construct a definition of integers, is that the failure of the norm equation to have a solution locally at any one prime is enough for the equation not to have solutions globally. Conversely, in order to have solutions globally, we need to be able to solve the norm equations locally at all primes. As already mentioned above, the reason we require c to be integral at q and equivalent to 1 mod q^3 is to make sure that factors of q do not ramify when we take the q-th root of c. Just making c have order divisible by q at all primes does not in general guarantee that factors of q do not ramify in such an extension. If any factor of q does ramify, then not all local units at this factor are norms in the extension, and making sure that the right side of the norm equation has order divisible by q at all primes might not be enough to guarantee a global solution. Hence we need to control the order of $c - 1$ at all factors of q at every level of the factor tree simultaneously, necessitating a stronger assumption on q than on other primes.

Depending on the field we might have a couple of options as far as integrality at q goes. If q happens to be completely p-bounded in our infinite extension for some $p \neq q$, then we can pretty much use the same method as above with the p-th root replacing the q-th root. The only difference is that, assuming we have the primitive p-th root of unity in the field, by definition of a complete p-boundedness, we can fix an element c of the field such that c is not a p-th power modulo any factor of q in any finite subextension of K_{inf} containing some fixed number field. We can also fix an element b of the field such that the order of b at any factor of q is not divisible by p in any finite subextension of K_{inf} containing the same fixed number field as above. Using such elements c and b we can get an existential definition of a subset of the field containing all elements with the order at any factor of q bounded from below by a bound depending on b and p. (See Proposition 3.9.) If ramification degrees of factors of q are altogether bounded, then we can arrange for this set to be the set of all field elements integral at factors of q, but in a general case the bound from below will be negative. In this case, to obtain the definition of integrality we will need one more step as described in Lemma 3.10.

Before going back to infinite extensions, we would like to make a brief remark about the sets definable by our methods over number fields. First of all, over any number field all primes are completely p-bounded for every p, and the ramification degree of factors of q is altogether bounded. So we can produce an existential and uniform (with parameters) definition of integrality at all factors of q. Note also that the complement of such a set is also uniformly existentially definable with parameters using the same method. So, in summary, we now obtain a uniform definition of the form $\forall\forall\exists\ldots\exists$ of the ring of integers of any number field with a q-th primitive root of unity. This result is along the lines of B. Poonen's result in [22], though his method is slightly different from ours since it uses ramified primes rather than non-splitting primes to obtain integrality formulas and restricts the discussion to $q = 2$ and quadratic forms. As B. Poonen, we can also use $q = 2$ and thus have a two-universal quantifier formula uniformly covering all number fields, but in this case if K has real embeddings, we need to make sure that c satisfies some additional conditions in order for the norm equations to have solutions (below we refer to these conditions as "making sure that $c \in \Omega_2(K)$").

Returning now to the case of infinite extensions, we note that, assuming q is p-bounded, we now have a uniform first-order definition with parameters of algebraic integers across all q-bounded algebraic extensions of $\mathbb{Q}$ where q is completely p-bounded. However, for the infinite case we may require more universal quantifiers. The number of these universal quantifiers will depend on whether the ramification degree of factors of q is bounded and on whether q has a finite number of factors.

The only case left to consider now is the case where q is not completely p-bounded for any $p \neq q$ but is completely q-bounded. This case requires a somewhat more technically complicated definition than the case where we had a requisite p. In particular, we still need a cyclic extension (once again of degree q), where all the factors of q will not split. Such an extension does exist, but we might have to extend our field to be in a position to take advantage of it. This construction is executed in Lemma 3.12.

2.4. Overview of our construction defining $\mathbb{Z}$ using finitely generated elliptic curves and one completely q-bounded prime. This section has an overview of a construction of a definition of a number field K over an infinite algebraic extension K_{inf} of $\mathbb{Q}$ using an elliptic curve with a Mordell–Weil group generated by points defined over K. This construction also requires one completely q-bounded prime p (which may equal q). Once we have a definition of K, a definition of $\mathbb{Z}$ follows from a result of J. Robinson. The theorem is stated below and will reappear with a proof as Theorem 6.5.

Theorem 2: *Let q be a rational prime and let K_{inf} be an infinite algebraic extension of $\mathbb{Q}$ with at least one prime of a number field contained in K_{inf} completely q-bounded. Assume also there exists an elliptic curve defined over*

K_{inf} such that its Mordell–Weil group has positive rank and is finitely generated. In this case $\mathbb{Z}$ is first-order definable over this field, and therefore the first-order theory of this field is undecidable.

The use of elliptic curves for the purposes of definability also has a long history, as long as the one for norm equations and quadratic forms. We review some of this history at the beginning of Section 6. Here we briefly dwell on the construction itself.

The main idea of the construction can be described as follows. Given an element $x \in K_{\mathrm{inf}}$, we write down a statement saying that x is integral at p and for every $n \in \mathbb{Z}_{>0}$ we have that x is equivalent to some element of K mod p^n. By the weak vertical method, this is enough to "push" x into K. (See Proposition 6.3.) Our elliptic curve is the source of elements of K. Any solution to an affine equation $y^2 = x^3 + ax + b$ of our elliptic curve must by assumption be in K. Further, if we let P be a point of infinite order and let the affine coordinates of $[n]P$ corresponding to our equation be (x_n, y_n), then the following statements are true:

(1) Let $\mathfrak{A}$ be any integral divisor of K and let m be a positive integer. Then there exists $k \in \mathbb{Z}_{>0}$ such that $\mathfrak{A} | \mathfrak{d}(x_{km})$, where $\mathfrak{d}(x_{km})$ is the denominator of the divisor of x_{km} in the integral divisor semigroup of K. (See Lemma 6.1.)

(2) There exists a positive integer m such that for any positive integers k, l,
$$\mathfrak{d}(x_{lm}) \Big| \mathfrak{n}\Big(\frac{x_{lm}}{x_{klm}} - k^2\Big)^2$$
in the integral divisor semigroup of K. Here $\mathfrak{d}(x_{lm})$ as above refers to the denominator of the divisor of x_{lm} and $\mathfrak{n}(\frac{x_{lm}}{x_{klm}} - k^2)$ refers to the numerator of the divisor of $\frac{x_{lm}}{x_{klm}} - k^2$. (See Lemma 6.2.)

Given $u \in K_{\mathrm{inf}}$ integral at some fixed K-prime $\mathfrak{p}_K$, we now consider a statement of the following sort: $\forall z \in K_{\mathrm{inf}}$ there exists $x, y, \hat{x}, \hat{y} \in K_{\mathrm{inf}}$ s.t. $(x, y), (\hat{x}, \hat{y})$ satisfy the chosen elliptic curve equation and both
$$\frac{1}{zx} \quad \text{and} \quad x\Big(u^2 - \frac{x}{\hat{x}}\Big)^2$$
are integral at $\mathfrak{p}_K$ implying that
$$\frac{(u^2 - \frac{x}{\hat{x}})^2}{z}$$
is integral at $\mathfrak{p}_K$.

If u satisfies this formula, then since $\frac{x}{\hat{x}} \in K$, by the weak vertical method we have that $u \in K$. Further, if u is a square of an integer, this formula can be satisfied. Thus we can proceed to define all integers, followed by all rational numbers and eventually K. Finally, being able to define $\mathbb{Z}$ implies undecidability of the first-order theory of the field.

2.5. Overview of the proof of undecidability of fields via undecidability of the rings of integers and $\mathscr{S}$-integers.

Our main undecidability results (reappearing later as Theorem 5.5, Corollary 5.7, Theorem 5.3, and Theorem 5.4 with proofs) are below:

Theorem 3: *Rational integers are first-order definable in any abelian extension of $\mathbb{Q}$ with finitely many ramified primes, and therefore the first-order theory of such fields is undecidable.*

Corollary 4: *Rational integers are first-order definable in the ring of integers of any abelian extension of $\mathbb{Q}$ with finitely many ramified primes, and therefore the first-order theory of such a ring is undecidable.*

Theorem 5: *Let q be a rational prime, let $m > 0$ be an integer and let*

$$K_{\inf} = \mathbb{Q}\left(\cos(2\pi/n), n = \prod_{i=1}^{s} p_i^{\ell_i}, p_i \not\equiv 1 \mod q^m, s, \ell_1, \ldots, \ell_s \in \mathbb{Z}_{>0} \right),$$

where p_i range over all primes satisfying the condition $p \not\equiv 1 \mod q^m$. In this case the first-order theory of $K_{\inf}$ is undecidable and $\mathbb{Z}$ is first-order definable $K_{\inf}$.

Theorem 6: *Any q-bounded totally real field is contained in a totally real field that has a first-order definition of rational integers and thus has an undecidable first-order theory.*

As K. Fukuzaki we obtain first-order undecidability results using results of J. Robinson for totally real fields. However, we are also able to use existential definability results previously obtained by the author to show that the first-order theory of fields and rings of integers of any abelian extension with finitely many ramified primes is undecidable, thus extending results of C. Videla. We also extend Videla's result by constructing a definition of $\mathbb{Z}$ in these extensions. (Videla constructed a model of $\mathbb{Z}$ to prove his undecidability results.) To be more specific, a result of J. Robinson implies that if a ring of integers has a certain invariant which C. Videla called a "Julia Robinson number", one can define a first-order model of $\mathbb{Z}$ over the ring. The Julia Robinson number s of a ring R of totally real integers is a real number s or ∞, such that $(0, s)$ is the smallest interval containing infinitely many sets of conjugates of numbers of R, i.e., infinitely many $x \in R$ with all the conjugates (over $\mathbb{Q}$) in $(0, s)$. A result of Kronecker implies that $s \geq 4$, and therefore if a totally real ring of integers in question contains the real parts of infinitely many distinct roots of unity, the Julia Robinson number for the ring is indeed 4, and we have the desired undecidability result.

To use the existential undecidability results for rings, we need to define the integral closures of the rings of $\mathscr{S}$-integers of number fields in infinite extensions under consideration. This construction is necessary because the existential undecidability results previously obtained by the author pertain only to these bigger rings and not to the rings of integers. The definitions of bigger rings require a minor adjustment of our construction above: we have to make c as above equivalent to 1 not just modulo q^3 but also modulo all the primes in $\mathscr{S}$. Further, as in the case of q and for similar reasons, we need primes in $\mathscr{S}$ to be completely q-bounded.

2.6. The structure of the paper. The paper is structured in the following manner. Most of the technical details of no independent interest are in the appendix (see Section 7). Section 3 constructs first-order definitions of the rings of algebraic integers in specified infinite algebraic extensions of $\mathbb{Q}$, and Section 4 contains various examples of fields satisfying the requirements for our definitions. Section 5 uses definitions of integers to produce undecidability results for fields. Finally, Section 6 explains how to use finitely generated elliptic curves to obtain definitions of rational integers.

Before we leave this section we establish notation to be used throughout the paper.

Notation and Assumptions 2.4: The following notation is used throughout the rest of the paper.

- Let q be a rational prime number.
- Let ξ_q be a primitive q-th root of unity.
- Let K, F, G, L denote algebraic extensions of $\mathbb{Q}$.
- For a number field G, let $\mathfrak{p}_G, \mathfrak{q}_G, \mathfrak{t}_G, \mathfrak{a}_G$ be distinct non-archimedean primes of G.

- If K is any finite extension of a number field G, then $\mathfrak{p}_K, \mathfrak{q}_K, \mathfrak{t}_K, \mathfrak{a}_K$ denote primes above $\mathfrak{p}_G, \mathfrak{q}_G, \mathfrak{t}_G, \mathfrak{a}_G$ respectively.
- For K and G as above, let $\mathscr{C}_K(\mathfrak{p}_G)$ denote the set of all K-primes above $\mathfrak{p}_G$.
- If K is a number field and $x \in K$ and $\operatorname{ord}_{\mathfrak{p}_K} x > 0$, we say by analogy with function fields that x has a zero at $\mathfrak{p}_K$. Similarly, if $\operatorname{ord}_{\mathfrak{p}_K} x < 0$, we say that x has a pole at $\mathfrak{p}_K$.
- If $\mathscr{S}_K$ is a set of non-archimedean primes of K, then we let $O_{K,\mathscr{S}_K}$ denote a subring of K containing all the elements of K without any poles at primes outside $\mathscr{S}_K$.
- Let $\tilde{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$.
- If K is a number field, then for any prime $\mathfrak{p}_K$, let $K_{\mathfrak{p}_K}$ be the completion of K under the $\mathfrak{p}_K$-adic topology.
- If K is a number field, and
$$\mathscr{S}_K = \{\mathfrak{p}_{1,K} \ldots, \mathfrak{p}_{l,K}\}$$
is a finite set of primes of K, then let $\Theta_q(K, \mathscr{S}_K)$ denote the set of all elements c of K such that the numerator of the divisor of $c-1$ is divisible by the divisor $\prod_{i=1}^{l} \mathfrak{p}_{i,K}$ in the semigroup of the integral divisors of K. If $\mathscr{S}_K = \emptyset$, then set $\Theta_q(K, \mathscr{S}_K) = K$.
- If K is a number field, let $\Phi_q(K)$ denote the set of all elements c of K such that the numerator of the divisor of $c - 1$ is divisible by q^3.
- If K is an infinite extension of $\mathbb{Q}$, and $\mathscr{S}_K$ is a set of valuations of K lying above finitely many primes of $\mathbb{Q}$, then a K-element c is in $\Theta_q(K, \mathscr{S}_K)$ if and only if for some number field $M \subset K$ and the set $\mathscr{S}_M$ of primes of M below valuations of $\mathscr{S}_K$ we have that $c \in \Theta_q(M, \mathscr{S}_M)$. Similarly, a K-element $c \in \Phi_q(K)$ if and only if $c \in \Phi_q(\mathbb{Q}(c))$.
- For an algebraic extension K of $\mathbb{Q}$, let $\Omega_2(K)$ be the set of all the elements c of K such that for any embedding σ of K into $\tilde{\mathbb{Q}}$ we have that $\sigma(K) \subset \mathbb{R} \cap \tilde{\mathbb{Q}}$ implies $\sigma(x) \geq 0$. If K has no real embeddings or $q > 2$, let $\Omega_q(K) = K$.

3. Defining the ring of integers in infinite extensions of $\mathbb{Q}$.

3.1. Local degree in infinite extensions. We start this section with a definition that will simplify the discussion below.

Definition 3.1: Given a G-prime $\mathfrak{p}_G$ and a field path $J_G = \{G - M_1 - M_2 \cdots\}$ from G to K_{inf}, as described in Notation 2.1, Part 4, call a path

$$\mathscr{P} = \{\mathfrak{p}_G - \mathfrak{p}_{M_1} - \mathfrak{p}_{M_2} \cdots\}$$

through the tree of $\mathfrak{p}_G$-factors q-**bounded**, if there exists $i \in \mathbb{Z}_{>0}$ such that for all integers $j \geq i$, we have that $\operatorname{ord}_q(d(\mathfrak{p}_{M_j}/\mathfrak{p}_G)) = \operatorname{ord}_q(d(\mathfrak{p}_{M_i}/\mathfrak{p}_G)) = n_i$. Also, call M_i a q-**bounding field** and call n_i a q-**bounding order**.

Remark 3.2: A q-bounding field and a q-bounding order also "work" off the field path where they were defined. Indeed, let M and n be a q-bounding field and order defined along some field path J_G, and let $N \in I_G$. In this case for some $\mathfrak{p}_N \in \mathscr{C}_N(\mathfrak{p}_G)$ it is true that $\operatorname{ord}_q(d(\mathfrak{p}_N/\mathfrak{p}_G)) \leq n$. Indeed, some field L along the field path J_G contains M and N and for some $\mathfrak{p}_L \in \mathscr{C}_L(\mathfrak{p}_G)$ we have that $\operatorname{ord}_q(d(\mathfrak{p}_L/\mathfrak{p}_G)) = n$. Thus, for $\mathfrak{p}_N = \mathfrak{p}_L \cap N \in \mathscr{C}_N(\mathfrak{p}_G)$ it is the case that $\operatorname{ord}_q(d(\mathfrak{p}_N/\mathfrak{p}_G)) \leq \operatorname{ord}_q(d(\mathfrak{p}_L/\mathfrak{p}_G)) = n$. Similarly, for any $L \in I_M$ we have that for some $\mathfrak{p}_L \in \mathscr{C}_L(\mathfrak{p}_M)$ it is the case that $\operatorname{ord}_q d(\mathfrak{p}_L/\mathfrak{p}_M) = 0$.

Lemma 3.3: *Choose any field path J_G as in Notation 2.1, Part 4 and consider the corresponding tree of factors for some prime $\mathfrak{p}_G$ of G. We claim that $\mathfrak{p}_G$ is q-bounded if and only if it lies along a q-bounded path.*

Proof. Indeed, suppose $\mathfrak{p}_G$ is q-bounded and let $n \in \mathbb{Z}_{>0}$ be such that for any $M \in J_G$ for some $\mathfrak{p}_M \in \mathscr{C}_M(\mathfrak{p}_G)$ we have that $d(\mathfrak{p}_M/\mathfrak{p}_G) \not\equiv 0 \mod q^n$. From the tree of $\mathfrak{p}_G$ factors corresponding to J_G remove all the "nodes" (i.e., factors of $\mathfrak{p}_G$) with the local degree with respect to $\mathfrak{p}_G$ divisible by q^n. Note that if a node survives removal, all of its predecessors must survive too. Thus, the tree structure is preserved under the removal of the nodes with the local degree with respect to $\mathfrak{p}_G$ divisible by q^n. This tree will have arbitrarily long paths and thus, by König's Lemma, an infinite path. Since the order at q of the local degree along this path is bounded, after some point the degree can grow only by factors prime to q.

Conversely, along a q-bounded path the order of the local degree at q will be bounded and therefore we cannot have arbitrarily large powers of q divide the local degree for all the factors of a prime on such a path. ∎

In the case a prime $\mathfrak{p}_G$ is completely q-bounded, by definition, there is a q-bounding field and a q-bounding order that work along all paths through the factor tree.

Definition 3.4: Let $\mathfrak{p}_G$ be a completely q-bounded prime and let $M \in I_G$ be such that for any $K \in I_M$, for any $\mathfrak{p}_M \in \mathscr{C}_M(\mathfrak{p}_G)$, and any $\mathfrak{p}_K \in \mathscr{C}_K(\mathfrak{p}_M)$ we have that $\operatorname{ord}_q d(\mathfrak{p}_K/\mathfrak{p}_M) = 0$. In this case call M a **completely q-bounding field** (for $\mathfrak{p}_G$). Call $\max_{\mathfrak{p}_M \in \mathscr{C}_M(\mathfrak{p}_G)}(\operatorname{ord}_q(d(\mathfrak{p}_M/\mathfrak{p}_G)))$ a **completely q-bounding order** (for $\mathfrak{p}_G$).

Our plan is to deal with all but finitely many primes first. This is accomplished in the section below.

3.2. The main part of the definition. We will use the following notation and assumptions in this section.

Notation and Assumptions 3.5:

- Let K_{inf} be an infinite algebraic extension of $\mathbb{Q}$.
- Let $G \subset K_{\text{inf}}$ be a number field, and let $\mathscr{S}_G$ be a finite, possibly empty set of primes of G. Suppose all the primes of G not dividing q and not in $\mathscr{S}_G$ are hereditarily q-bounded in K_{inf}.
- Let $\mathscr{Q}_G$ be the set of all factors of q in G.
- Let $\mathscr{W}_G = \mathscr{S}_G \cup \mathscr{Q}_G$.
- Let $O_{K_{\text{inf}},\mathscr{W}_{K_{\text{inf}}}}, O_{K_{\text{inf}},\mathscr{S}_{K_{\text{inf}}}}, O_{K_{\text{inf}},\mathscr{Q}_{K_{\text{inf}}}}$ denote the integral closure of $O_{G,\mathscr{W}_G}$, $O_{G,\mathscr{S}_G}$ and $O_{G,\mathscr{Q}_G}$ respectively in K_{inf}.

Proposition 3.6: *If $\xi_q \in G$, $b, x \in K_{\text{inf}}$, $x \neq 0, bx^q + b^q \neq 0$*

$$c \in \Omega_q(K_{\text{inf}}) \cap \Phi_q(K_{\text{inf}}) \cap \Theta_q(K, \mathscr{S}_{K_{\text{inf}}}),$$

and there exists $y \in L_{\text{inf}}$, where

$$L_{\text{inf}} = K_{\text{inf}}(\sqrt[q]{1 + x^{-1}}, \sqrt[q]{1 + (bx^q + b^q)^{-1}}, \sqrt[q]{1 + (c + c^{-1})x^{-1}})$$

such that

$$\mathbf{N}_{L_{\text{inf}}(\sqrt[q]{c})/L_{\text{inf}}}(y) = bx^q + b^q, \tag{3.2}$$

then there exists a field $M \in I_G$ such that for any field $K \in I_M$, for any non-archimedean prime $\mathfrak{p}_K$ of K not in $\mathscr{W}_K$, one of the following conditions holds:

1. *c is a q-th power mod $\mathfrak{p}_K$, or*
2. *$\operatorname{ord}_{\mathfrak{p}_K} x \geq 0$, or*
3. *$q \operatorname{ord}_{\mathfrak{p}_K} x \geq (q-1) \operatorname{ord}_{\mathfrak{p}_K} b$, or*
4. *$\operatorname{ord}_{\mathfrak{p}_K} b \equiv 0 \mod q$.*

At the same time, if $x \in O_{K_{\text{inf}},\mathscr{W}_{K_{\text{inf}}}}$, then (3.2) has a solution $y \in L_{\text{inf}}$.

Proof. Suppose that (3.2) holds for some x, b, c, y as specified above. Let $M \in I_G$ be such that

$$x, b, c \in M, \tag{3.3}$$

$$y \in L_M(\sqrt[q]{c}), \tag{3.4}$$

where

$$L_M = M(\sqrt[q]{1 + x^{-1}}, \sqrt[q]{1 + (bx^q + b^q)^{-1}}, \sqrt[q]{1 + (c + c^{-1})x^{-1}})$$

and

$$[L_{\inf}(\sqrt[q]{c}) : L_{\inf}] = [L_M(\sqrt[q]{c}) : L_M]. \tag{3.5}$$

In this case, for any $K \in I_M$, we also have that $x, b, c \in K$, $y \in L_K(\sqrt[q]{c})$, where

$$L_K = K(\sqrt[q]{1 + x^{-1}}, \sqrt[q]{1 + (bx^q + b^q)^{-1}}, \sqrt[q]{1 + (c + c^{-1})x^{-1}})$$

with

$$[L_{\inf}(\sqrt[q]{c}) : L_{\inf}] = [L_K(\sqrt[q]{c}) : L_K],$$

and therefore it is also the case

$$\mathbf{N}_{L_K(\sqrt[q]{c})/L_K}(y) = bx^q + b^q. \tag{3.6}$$

Now, if for some K-prime $\mathfrak{p}_K$ such that $\mathfrak{p}_K \notin \mathscr{W}_K$ we have that none of the Conditions (1)–(4) is satisfied, then by Proposition 7.9 we have that

$$\operatorname{ord}_{\mathfrak{p}_{L_K}}(bx^q + b^q) \not\equiv 0 \mod q$$

and c is not a q-th power modulo $\mathfrak{p}_{L_K}$. Hence by Lemma 7.7 we conclude that the norm equation (3.6) has no solution in $L_K(\sqrt[q]{c})$ contradicting our assumptions.

Suppose now that

$$x \in O_{K_{\inf}, \mathscr{W}_{K_{\inf}}},$$

let $M \in I_G$ satisfy assumptions (3.3), (3.5) and be such that

$$c \in \Omega_q(M) \cap \Phi_q(M) \cap \Theta_q(M, \mathscr{S}_M).$$

(We can find M satisfying $c \in \Omega_q(M)$ by Remark 7.3.) We now choose any $K \in I_M$ and show that (3.6) has a solution $y \in L_K(\sqrt[q]{c})$. Since (3.5) ensures that for any $y \in L_K(\sqrt[q]{c})$,

$$\mathbf{N}_{L_K(\sqrt[q]{c})/L_K}(y) = \mathbf{N}_{L_{\inf}(\sqrt[q]{c})/L_{\inf}}(y), \tag{3.7}$$

we need to solve

$$\mathbf{N}_{L_K(\sqrt[q]{c})/L_K}(y) = bx^q + b^q$$

only.

Since $x \in O_{K_{\rm inf}, \mathscr{W}_{K_{\rm inf}}}$, we have that $x \in O_{K, \mathscr{W}_K}$. Further, we also have that

$$c \in \Omega_q(K) \cap \Phi_q(K) \cap \Theta_q(K, \mathscr{S}_K),$$

by definition of these sets and Remark 7.3. In this case by Proposition 7.10, for every prime $\mathfrak{a}_{L_K}$ not dividing q or any prime in $\mathscr{S}_K$, we have the following:

- $\operatorname{ord}_{\mathfrak{a}_{L_K}}(bx^q + b^q) \equiv 0 \mod q$, and
- $\operatorname{ord}_{\mathfrak{a}_{L_K}} c \equiv 0 \mod q$.

Further, by Lemma 7.8 and by our assumption that $c \in \Phi_q(K)$, we know that factors of q are not ramified in the extension $L_K(\sqrt[q]{c})/L_K$, and since the divisor of c is a q-th power in L_K, the extension $L_K(\sqrt[q]{c})/L_K$ is unramified at all finite primes by Lemma 7.6.

By Hasse's Norm Principle (see Theorem 32.9 of [24]) this norm equation has solutions globally (i.e., in $L_K(\sqrt[q]{c})$) if and only if it has a solution locally (i.e., in every completion).

Observe further that locally every unit is a norm in an unramified extension (see Proposition 6, Section 2, Chapter XII of [44]), and we do not have to worry about archimedean primes, given our assumption on c. Indeed, if $q > 2$, then K has no embeddings into $\mathbb{R}$ and therefore all the archimedean completions of all the fields involved are isomorphic to $\mathbb{C}$. If $q = 2$, then we have to worry about one possibility only: an archimedean completion of L_K is isomorphic to $\mathbb{R}$, while a corresponding archimedean completion of $L_K(\sqrt{c})$ is isomorphic to $\mathbb{C}$. However, this case is precluded by Lemma 7.13 and our assumption that $c \in \Omega_q(K)$.

Next we observe that since $L_K(\sqrt[q]{c})/L_K$ is a cyclic extension of prime degree, by Lemma 7.7 every unramified prime either splits completely or does not split at all. If a prime splits completely, then the local degree is one and every element of the field below is automatically a norm locally at this prime. So the only primes where we might have elements that are not local norms are the primes that do not split, or, in other words, the primes where the local degree is q. (Note that any factor of q and any factor of a prime in $\mathscr{S}_K$ split completely in the extension $L_K(\sqrt[q]{c})/L_K$ by our assumptions on c and Lemmas 7.6 and 7.8.)

So let $\mathfrak{r}_{L_K}$ be a prime of local degree q not in $\mathscr{W}_{L_K}$. By the argument above we have that $\operatorname{ord}_{\mathfrak{r}_{L_K}}(bx^q + b^q) \equiv 0 \mod q$. In this case, by the Weak Approximation Theorem, there exists $u \in L_K$ such that $\operatorname{ord}_{\mathfrak{r}_{L_K}} u = 1$ and therefore for some integer m it is the case that $u^{qm}(bx^q + b^q)$ has order 0 at $\mathfrak{r}_{L_K}$ or in other words $u^{qm}(bx^q + b^q)$ is a unit at $\mathfrak{r}_{L_K}$.

As any q-th power of an L_K-element, u^{mq} is a norm locally since the degree of the local extension is q by our assumption. Therefore, $u^{mq}(bx^q+b^q)$ is a norm at $\mathfrak{r}_{L_K}$ if and only if (bx^q+b^q) is a norm at $\mathfrak{r}_{L_K}$. But $u^{mq}(bx^q+b^q)$ is a unit at $\mathfrak{r}_{L_K}$ and therefore is a norm. Hence bx^q+b^q is a norm. ∎

Corollary 3.7: *If $\xi_q \in G$ then*

$$\begin{aligned} O_{K_{\inf},\mathscr{W}_{K_{\inf}}} = \{0\} \cup \{x \in K_{\inf} \setminus \{0\} | \forall c \in \Theta_q(K_{\inf}, \mathscr{S}_{K_{\inf}}) \cap \Phi_q(K_{\inf}) \cap \Omega_q(K_{\inf}) \\ \forall b \in K_{\inf} \\ ((bx^q + b^q = 0) \vee \exists y \in L_{\inf}(\sqrt[q]{c}) : \\ \mathbf{N}_{L_{\inf}(\sqrt[q]{c})/L_{\inf}}(y) = bx^q + b^q)\}. \end{aligned} \tag{3.8}$$

In particular, if $\mathscr{S}_{K_{\inf}}$ is empty, then

$$\begin{aligned} O_{K_{\inf},\mathscr{Q}_{K_{\inf}}} = \{0\} \cup \{x \in K_{\inf} \setminus \{0\} | \forall c \in \Phi_q(K_{\inf}) \cap \Omega_q(K_{\inf}) \\ \forall b \in K_{\inf} \\ ((bx^q + b^q = 0) \vee \exists y \in L_{\inf}(\sqrt[q]{c}) : \\ \mathbf{N}_{L_{\inf}(\sqrt[q]{c})/L_{\inf}}(y) = bx^q + b^q)\}, \end{aligned} \tag{3.9}$$

and if additionally $q > 2$ or $K_{\inf}$ has no real embeddings, then

$$\begin{aligned} O_{K_{\inf},\mathscr{Q}_{K_{\inf}}} = \{0\} \cup \{x \in K_{\inf} \setminus \{0\} | \forall c \in \Phi_q(K_{\inf}) \\ \forall b \in K_{\inf} \\ ((bx^q + b^q = 0) \vee \exists y \in L_{\inf}(\sqrt[q]{c}) : \\ \mathbf{N}_{L_{\inf}(\sqrt[q]{c})/L_{\inf}}(y) = bx^q + b^q)\}. \end{aligned} \tag{3.10}$$

Proof. The only assertion that requires proof is that if $x \notin O_{K_{\inf},\mathscr{W}_{K_{\inf}}}$ then there exist $b, c \in K_{\inf}$, as specified in (3.8), for which (3.2) has no solution $y \in L_{\inf}(\sqrt[q]{c})$.

If $x \notin O_{K_{\inf},\mathscr{W}_{K_{\inf}}}$, then for some prime $\mathfrak{p}_{G(x)} \notin \mathscr{W}_{G(x)}$ we have that

$$\operatorname{ord}_{\mathfrak{p}_{G(x)}} x < 0,$$

$$\mathfrak{p}_G = \mathfrak{p}_{G(x)} \cap G \notin \mathscr{W}_G$$

and $\mathfrak{p}_G$ is herediterily q-bounded in $K_{\inf}$. Thus, $\mathfrak{p}_{G(x)}$ is q-bounded in $K_{\inf}$. Let $M \in I_{G(x)}$ be any field containing a q-bounding field for $\mathfrak{p}_{G(x)}$ and note that by the Strong Approximation Theorem there exists

$$c \in \Theta_q(M, \mathscr{S}_M) \cap \Phi_q(M) \cap \Omega_q(M) \subset \Theta_q(K_{\inf}, \mathscr{S}_{K_{\inf}}) \cap \Phi_q(K_{\inf}) \cap \Omega_q(K_{\inf})$$

such that c is not a q-th power modulo $\mathfrak{p}_M$, where $\mathfrak{p}_M \in \mathscr{C}_M(\mathfrak{p}_{G(x)})$ lies along the q-bounded path for which M is a q-bounding field. Further, let $b \in M$ such that $\operatorname{ord}_{\mathfrak{p}_M} b = -1$ and thus $q \operatorname{ord}_{\mathfrak{p}_M} x < (q-1)\operatorname{ord}_{\mathfrak{p}_M} b$. Observe further that for any $K \in I_M$ we also have that

(1) $c \in \Omega_q(K) \cap \Phi_q(K) \cap \Theta_q(K, \mathscr{S}_K)$, by definition of sets $\Omega_q(K), \Phi_q(K)$, and $\Theta_q(K, \mathscr{S}_K)$,

(2) for at least one $\mathfrak{p}_K \in \mathscr{C}_K(\mathfrak{p}_M)$ we have that $d(\mathfrak{p}_K/\mathfrak{p}_M)$ and therefore $f(\mathfrak{p}_K/\mathfrak{p}_M)$ are not divisible by q by definition of a q-bounding field, and therefore c is not a q-th power modulo at least one $\mathfrak{p}_K \in \mathscr{C}_K(\mathfrak{p}_M)$,

(3) for the same $\mathfrak{p}_K$ as in (2) we also have that $e(\mathfrak{p}_K/\mathfrak{p}_M)$ is not divisible by q, and therefore $\operatorname{ord}_{\mathfrak{p}_K} b \not\equiv 0 \mod q$ while $q \operatorname{ord}_{\mathfrak{p}_K} x < (q-1)\operatorname{ord}_{\mathfrak{p}_K} b$.

Thus none of Conditions (1)–(4) of Proposition 3.6 is satisfied for any $K \in I_M$. So M as required by Proposition 3.6 does not exist, and hence (3.2) has no solution $y \in L_{\text{inf}}$. ∎

3.3. Integrality at finitely many primes using complete p-boundedness for $p \neq q$.

We now consider definitions of integrality at finitely many primes to define $\Theta_q(K_{\text{inf}}, \mathscr{S}_{K_{\text{inf}}})$, $\Phi_q(K_{\text{inf}})$ and their complements. One way to do this is to use a bit of "circular reasoning" by introducing another rational prime p into the picture and making additional assumptions about our field. (Here "circular reasoning" refers to the fact that we use q to define integrality at factors of p, and we use p to define integrality at factors of q.)

Notation and Assumptions 3.8:

- Let $p \neq q$ (with q as above) be a rational prime.
- Assume $\xi_p \in G$.
- Assume factors of q and primes in $\mathscr{S}_G$ are *completely p-bounded* in K_{inf} and are all prime to p.
- Let $\mathscr{W}_G = \mathscr{S}_G \cup \{\text{factors of } q \text{ in } G\}$, as above.
- Let $M_p \in I_G$ be a completely p-bounding field for *all* primes in $\mathscr{W}_G$. (Even though completely bounding fields were defined for a single prime, clearly any finite collection of completely bounded primes has a common completely bounding field, a field that contains a completely bounding field for each prime in the set.)

Proposition 3.9: *Let $d \in M_p$ be such that the denominator of its divisor is divisible by every prime of $\mathscr{W}_{M_p}$ and d has no other poles. Assume further that for any $\mathfrak{p}_{M_p} \in \mathscr{W}_{M_p}$ it is the case that $\operatorname{ord}_{\mathfrak{p}_{M_p}} d \not\equiv 0 \mod p$. (Note that such an element $d \in M_p$ exists by the Strong Approximation Theorem.) Let $a \in \Phi_p(M_p) \cap \Omega_p(M_p)$, and let a be equivalent to a non-p-th power element of the residue field modulo any prime of $\mathscr{W}_{M_p}$. (Existence of a is also guaranteed by the Strong Approximation Theorem.) Now let*

$$N_{\inf} = K_{\inf}(\sqrt[p]{1+d^{-1}}, \sqrt[p]{1+(dx^p+d^p)^{-1}}, \sqrt[p]{1+(a+a^{-1})d^{-1}})$$

and let

$$B(K_{\inf}, p, a, d) = \{x \in K_{\inf} | \exists y \in N_{\inf}(\sqrt[p]{a}) : \mathbf{N}_{N_{\inf}(\sqrt[p]{a})/N_{\inf}}(y) = dx^p + d^p\}.$$

We claim

$$B(K_{\inf}, p, a, d) = \{x \in K_{\inf} | \forall K \in I_{M_p(x)} \forall \mathfrak{p}_K \in \mathscr{W}_K : \operatorname{ord}_{\mathfrak{p}_K} x > \frac{p-1}{p} \operatorname{ord}_{\mathfrak{p}_K} d\}.$$

Proof. The proof of the proposition is almost identical to the proof of Proposition 3.6. One should only point out the following two adjustments.

(1) By construction, no pole of d in any $K \in I_{M_p}$ occurs in the divisor of a, since a is not a p-th power modulo primes of $\mathscr{W}_K$. Thus, $(a + a^{-1})d^{-1}$ has poles at all the primes occurring in the divisor of a. Also, all zeros of d of orders not divisible by p in K are ramified with ramification degree p before we adjoin $\sqrt[p]{1+(a+a^{-1})d^{-1}}$, and therefore in

$$N_K = K(\sqrt[p]{1+d^{-1}}, \sqrt[p]{1+(dx^p+d^p)^{-1}}, \sqrt[p]{1+(a+a^{-1})d^{-1}})$$

all zeros and poles of a have order divisible by p.

(2) For any prime $\mathfrak{p}_K \in \mathscr{W}_K$ we have that

$$\operatorname{ord}_{\mathfrak{p}_K}(dx^p) \neq \operatorname{ord}_{\mathfrak{p}_K}(d^p),$$

since the left order is not equivalent to 0 mod p and the right one is. Thus under these circumstances, $\operatorname{ord}_{\mathfrak{p}_K}(dx^p + d^p) \equiv 0 \mod p$ implies that $\operatorname{ord}_{\mathfrak{p}_K}(dx^p + d^p) = \operatorname{ord}_{\mathfrak{p}_K}(d^p)$ and

$$\operatorname{ord}_{\mathfrak{p}_K} x > \frac{p-1}{p} \operatorname{ord}_{\mathfrak{p}_K} d > \operatorname{ord}_{\mathfrak{p}_K} d. \tag{3.11}$$

Conversely, if for some $K \in I_{M_p(x)}$ we have that (3.11) holds for all K-primes above primes of $\mathscr{W}_G$, then $\operatorname{ord}_{\mathfrak{p}_K}(dx^p + d^p) \equiv 0 \mod p$ and $x \in B(K_{\inf}, p, a, d)$. ∎

We now use this definition of $B(K_{\text{inf}}, p, a, d)$ to obtain a definition of $R_{K_{\text{inf}},\mathscr{W}_{\text{inf}}}$—the ring of elements of K_{inf} integral with respect to primes of $\mathscr{W}_G$. To do this we note the following.

Lemma 3.10:

$$R_{K_{\text{inf}},\mathscr{W}_{\text{inf}}} = \{x \in B(K_{\text{inf}}, p, a, d) | \forall y \in B(K_{\text{inf}}, p, a, d) : xy \in B(K_{\text{inf}}, p, a, d)\}.$$

Proof. First assume that $x \in R_{K_{\text{inf}},\mathscr{W}_{\text{inf}}} \subset B(K_{\text{inf}}, p, a, d)$ and note that in this case x has non-negative order at all primes of $\mathscr{W}_{G(x)}$. Thus, if for some field $K \in I_{G(x)}$ and some K-prime $\mathfrak{p}_K$ above a prime of $\mathscr{W}_G$ we have that

$$\text{ord}_{\mathfrak{p}_K} y > \frac{p-1}{p} \text{ord}_{\mathfrak{p}_K} d,$$

then

$$\text{ord}_{\mathfrak{p}_K} xy \geq \text{ord}_{\mathfrak{p}_K} y > \frac{p-1}{p} \text{ord}_{\mathfrak{p}_K} d.$$

Conversely, suppose that $x \in B(K_{\text{inf}}, p, a, d) \setminus R_{K_{\text{inf}},\mathscr{W}_{\text{inf}}}$ and note that in $K = M_p(x)$ we must have for some K-prime $\mathfrak{p}_K$ above a prime of $\mathscr{W}_G$ that

$$\frac{p-1}{p} \text{ord}_{\mathfrak{p}_K} d < \text{ord}_{p} x < 0.$$

Therefore there exists an $r \in \mathbb{Z}_{\geq 1}$ such that

$$x^r \in B(K_{\text{inf}}, p, a, d)$$

but

$$x^{r+1} \notin B(K_{\text{inf}}, p, a, d).$$

Hence if we set $y = x^r$, we see that $y \in B(K_{\text{inf}}, p, a, d)$ but $xy \notin B(K_{\text{inf}}, p, a, d)$. ∎

3.4. Defining Integrality at finitely many primes using complete q-boundedness. Our next step is to show that we can get away using q-boundedness only (without introducing p-boundedness for an additional prime p). The integrality at primes of $\mathscr{S}_{K_{\text{inf}}}$ can be handled with complete q-boundedness only using sets $B(K_{\text{inf}}, q, a, d)$ for appropriately selected a and d as above, since the primes of $\mathscr{S}_K$ are not factors of q. Thus we need to make special arrangements for factors of q only. Since we are going to use q-boundedness exclusively, we now drop Assumptions and Notation 3.8 and introduce the following assumptions and notation.

Notation and Assumptions 3.11: We will use the following notation and assumptions.

- Assume all the primes of $\mathscr{W}_G$ are completely q-bounded.
- Let M_q be a completely q-bounding field for all primes in $\mathscr{W}_G$.
- Assume $\xi_q \in G$.
- Let $\mathscr{Q}_G$ be the set of all factors of q in G.
- Let $f_q = \max_{\mathfrak{q}_{M_q} \in \mathscr{Q}_{M_q}} \{f(\mathfrak{q}_{M_q}/q)\}$.
- Let $F/\mathbb{Q}$ be a totally real cyclic extension of degree q^{f_q+1}, where q does not split. (Such an extension exists by Lemma 7.16.)

Now consider a cyclic extension $FK_{\inf}/K_{\inf}$ of degree q^r (this extension is cyclic of degree equal to a power of q by Lemma 7.17), where $0 \leq r \leq f_q + 1$. We claim that in fact $r > 0$. Assume the opposite. In this case for some $K \in I_{M_q}$ we have that $F \subseteq K$. But the relative degree of any factor of q in K is at most f_q, while the relative degree of all the factors of q in FK is bigger than f_q. Thus, $r > 0$.

Now let $E_{\inf}$ be the unique subfield of $FK_{\inf}$ such that $[FK_{\inf} : E_{\inf}] = q$ and $K_{\inf} \subset E_{\inf}$. Since $\xi_q \in E_{\inf}$, we must have $FK_{\inf} = E_{\inf}(\sqrt[q]{a})$ for some $a \in E_{\inf}$ (this is so by Theorem 6.2, page 288 of [14]). Let $\beta \in E_{\inf}$ generate $E_{\inf}$ over $K_{\inf}$. Now let $N \in I_{M_q}$ be such that $F \subset N(\sqrt[q]{a}, \beta)$, $a \in N(\beta)$, and β is of the same degree over N as over $K_{\inf}$. Let $K \in I_N$ and note that β is of the same degree over K as over N, $a \in K(\beta)$, and $F \subset K(\sqrt[q]{a}, \beta)$. Further, $KF = K(\sqrt[q]{a}, \beta)/K$ is a cyclic extension of degree q^r for some $r > 0$, no factor of q ramifies in this extension (by Proposition 8 of Chapter II, §4 of [13]), and no factor of q splits in the extension $K(\sqrt[q]{a}, \beta)/K(\beta)$ by Lemma 7.18. By Lemma 7.20 we can also assume $a \in \Omega_q(K(b))$.

Since factors of q in $N(\beta)$ do not ramify in the extension $N(\beta, \sqrt[q]{a})/N(\beta)$, if for some factor $\mathfrak{q}_{N(\beta)}$ of q in $N(\beta)$ we have that $\operatorname{ord}_{\mathfrak{q}_{N(\beta)}} a \neq 0$, we also must have $\operatorname{ord}_{\mathfrak{q}_{N(\beta)}} a \equiv 0 \mod q$. Thus without loss of generality (multiplying a by q-th powers of some elements of $N(\beta)$, if necessary), we can assume that a has no occurrences of factors of q in its divisor. Note that if $q = 2$, we would only be multiplying a by squares and thus not changing the fact that $a \in \Omega_2(N(\beta))$.

Now let $\mathscr{A}_{N(\beta)} \subseteq \mathscr{C}_{N(\beta)}(q) = \mathscr{Q}_{N(\beta)}$ and let $d \in N(\beta)$ be such that for all primes $\mathfrak{q}_{N(\beta)} \in \mathscr{A}_{N(\beta)}$ we have that

$$\operatorname{ord}_{\mathfrak{q}_{N(\beta)}} d \not\equiv 0 \mod q, \quad \operatorname{ord}_{\mathfrak{q}_{N(\beta)}} d \leq -3 \operatorname{ord}_{\mathfrak{q}_{N(\beta)}} q$$

and d has no other poles. As above, such a d exists by the Strong Approximation Theorem.

The reason for possibly choosing a subset of factors of q is to point out that in principle we don't have to treat all the factors of q the same way, i.e., we may want to allow some of the factors in "denominators", while banning others. The proposition below lets us bound the order of the poles the elements of our field can have at factors of q in $\mathscr{A}_{N(\beta)}$, while imposing no constraints on other factors of q.

Proposition 3.12: *Let E_{inf} be defined as above, let*

$$F_{\mathrm{inf}} = E_{\mathrm{inf}}(\sqrt[q]{1+d^{-1}}, \sqrt[q]{1+(dx^p+d^p)^{-1}}, \sqrt[q]{1+(a+a^{-1})d^{-1}}),$$

and let

$$C(E_{\mathrm{inf}}, a, d, q) = \{x \in K_{\mathrm{inf}} | \exists y \in F_{\mathrm{inf}}(\sqrt[q]{a}) : \mathbf{N}_{F_{\mathrm{inf}}(\sqrt[q]{a})/F_{\mathrm{inf}}}(y) = dx^q + d^q\}.$$

We claim

$$C(E_{\mathrm{inf}}, a, d, q) = \Big\{x \in K_{\mathrm{inf}} | \forall K \in I_{N(\beta,x)}\, \forall \mathfrak{q}_K \in \mathscr{A}_K : \mathrm{ord}_{\mathfrak{q}_K} x > \frac{q-1}{q} \mathrm{ord}_{\mathfrak{q}_K} d\Big\}.$$

Proof. The proof of this proposition is almost identical to the proof of Proposition 3.9 except that it relies on Proposition 7.11 and Proposition 7.12 in lieu of Proposition 7.9 and Proposition 7.10. ∎

As above, Lemma 3.10 allows us to use the definition of $C(E_{\mathrm{inf}}, a, d, q)$ to obtain a definition $R_{K_{\mathrm{inf}}, \mathscr{A}_{\mathrm{inf}}}$. With the definition of $R_{K_{\mathrm{inf}}, \mathscr{A}_{\mathrm{inf}}}$ in mind, we now modify slightly the definition in Corollary 3.7 to replace

$$\Phi_q(K_{\mathrm{inf}}, \mathscr{S}_{K_{\mathrm{inf}}}) \cap \Phi_q(K_{\mathrm{inf}})$$

with an expression involving $R_{K_{\mathrm{inf}}, \mathscr{W}_{\mathrm{inf}}}$. We also state the corresponding definitions of $O_{K_{\mathrm{inf}}, \mathscr{S}_{K_{\mathrm{inf}}}}$ for the case where $\mathscr{S}_G \cap \mathscr{Q}_G = \emptyset$, and $O_{K_{\mathrm{inf}}}$. Let $w, \hat{w} \in G$ be such that

1. $\mathrm{ord}_{\mathfrak{q}_G} w = 3 \,\mathrm{ord}_{\mathfrak{q}_G} q$ for any $\mathfrak{q}_G \in \mathscr{C}_G(q)$,
2. $\mathrm{ord}_{\mathfrak{p}_G} w = 1$ for any $\mathfrak{p}_G \in \mathscr{S}_G$,
3. w has no other zeros,
4. $\mathrm{ord}_{\mathfrak{q}_G} \hat{w} = 3 \,\mathrm{ord}_{\mathfrak{q}_G} q$ for any $\mathfrak{q}_G \in \mathscr{C}_G(q)$,
5. $\hat{w}$ has no other zeros.

(As above, such elements w and $\hat{w}$ exist by the Strong Approximation Theorem.)

Corollary 3.13:

(1) $x \in O_{K_{\mathrm{inf}},\mathscr{W}_{K_{\mathrm{inf}}}}, x \neq 0$

$$\Leftrightarrow \forall c \textit{ such that } \Big(\frac{(c-1)}{w} \in R_{K_{\mathrm{inf}},\mathscr{W}_{\mathrm{inf}}} \wedge c \in \Omega_q(K_{\mathrm{inf}})\Big)$$
$$\forall b \in K_{\mathrm{inf}}((bx^q + b^q = 0) \vee \exists y \in L_{\mathrm{inf}}(\sqrt[q]{c}) :$$
$$\mathbf{N}_{L_{\mathrm{inf}}(\sqrt[q]{c})/L_{\mathrm{inf}}}(y) = bx^q + b^q).$$

(2) $x \in O_{K_{\mathrm{inf}},\mathscr{S}_{K_{\mathrm{inf}}}}, x \neq 0$

$$\Leftrightarrow x \in R_{K_{\mathrm{inf}},\mathscr{Q}_{\mathrm{inf}}}$$
$$\wedge \forall c \textit{ such that } \Big(\frac{(c-1)}{w} \in R_{K_{\mathrm{inf}},\mathscr{W}_{\mathrm{inf}}} \wedge c \in \Omega_q(K_{\mathrm{inf}})\Big)$$
$$\forall b \in K_{\mathrm{inf}}((bx^q + b^q = 0) \vee \exists y \in L_{\mathrm{inf}}(\sqrt[q]{c}) :$$
$$\mathbf{N}_{L_{\mathrm{inf}}(\sqrt[q]{c})/L_{\mathrm{inf}}}(y) = bx^q + b^q).$$

(3) $x \in O_{K_{\mathrm{inf}}}, x \neq 0$

$$\Leftrightarrow x \in R_{K_{\mathrm{inf}},\mathscr{Q}_{\mathrm{inf}}}$$
$$\wedge \forall c \textit{ such that } \Big(\frac{(c-1)}{\hat{w}} \in R_{K_{\mathrm{inf}},\mathscr{Q}_{\mathrm{inf}}} \wedge c \in \Omega_q(K_{\mathrm{inf}})\Big)$$
$$\forall b \in K_{\mathrm{inf}}((bx^q + b^q = 0) \vee \exists y \in L_{\mathrm{inf}}(\sqrt[q]{c}) :$$
$$\mathbf{N}_{L_{\mathrm{inf}}(\sqrt[q]{c})/L_{\mathrm{inf}}}(y) = bx^q + b^q).$$

Proof. We show that the first formula defines the right set. The argument for the other two definitions is similar. It is enough to observe the following. In any $K \in I_N$ the numerator of the divisor of $c-1$ is divisible by the numerator of the divisor of q^3 and by every $\mathfrak{p}_K$ in $\mathscr{S}_K$. Thus $c \in \Theta_q(K,\mathscr{S}_K) \cap \Phi_q(K)$. Conversely, if $c \in \Theta_q(K,\mathscr{S}_K) \cap \Phi_q(K)$, then the divisor $c-1$ is divisible by the numerator of the divisor of q^3 and by every $\mathfrak{p}_K$ in $\mathscr{S}_K$ and therefore $\frac{c-1}{w}$ does not have any poles at primes of $\mathscr{W}_K$, so that

$$\frac{(c-1)}{w} \in R_{K_{\mathrm{inf}},\mathscr{W}_{\mathrm{inf}}}. \qquad \blacksquare$$

Theorem 3.14: *Let p, q be rational prime numbers, not necessarily distinct. Let H be a number field, and let H_{inf} be an algebraic extension of H. Let $\mathscr{S}_H$ be a finite, possibly empty, set of primes of H. Assume all primes of H not in $\mathscr{S}_H$ are hereditarily q-bounded in H_{inf}, and primes in $\mathscr{S}_H$ and factors of q are completely p-bounded in H_{inf}. In this case, the integral closure of $O_{H,\mathscr{S}_H}$ in H_{inf} is first-order definable over H_{inf}.*

Proof. Given an arbitrary number field H and an algebraic extension H_{inf} of H, not necessarily containing any roots of unity required above, we have to show that the norm equations we have been using in our definitions can be rewritten as polynomial equations with relevant solutions in H_{inf}. Below we present an informal outline of this rewriting process. For a more general and formal discussion of the rewriting techniques we refer the reader to the section on coordinate polynomials in [34]. Let $G = H(\xi_q, \xi_p), K_{\text{inf}} = H_{\text{inf}}(\xi_q, \xi_p)$.

We start with rewriting the norm equation itself. If T is any field of characteristic 0 and $c \in T \setminus T^q$, $u_1, \ldots, u_q, z \in T$, $y = \sum_{i=1}^{q} a_i \sqrt[q]{c}^{(i-1)}$, then

$$\begin{aligned}\text{(3.12)} \qquad \mathbf{N}_{T(\sqrt[q]{c})/T}(y) - z = &\prod_{j=0}^{q-1}\sum_{i=1}^{q} u_i \xi_q^{(i-1)j} \sqrt[q]{c}^{(i-1)} - z \\ =&N(u_1, \ldots, u_q, c, z) \in \mathbb{Z}[u_1, \ldots, u_q, c, z],\end{aligned}$$

and the coefficients of $N(U_1, \ldots, U_q, C, Z)$ depend on q only.

If $c, w \in T, c = w^q$, then for any $z \in T$ the equation $N(U_1, \ldots, U_q, c, z) = 0$ has solutions $u_1, \ldots, u_q \in T(\xi_q)$. Indeed, consider the following system of equations:

$$\begin{cases} \sum_{i=0}^{q-1} u_i w^i = z, \\ \sum_{i=0}^{q-1} u_i \xi_q^{ij} w^i = 1, \quad j = 1, \ldots, q-1. \end{cases}$$

This is a nonsingular system with a matrix $(\xi_q^{ij} w^i)$, $i = 0, \ldots, q-1$, $j = 0, \ldots, q-1$ having all of its entries in $T(\xi_q)$. Since the vector $(z, 1, \ldots, 1)$ also has all of its entries in $T(\xi_q)$, we conclude that the system has a unique solution in $T(\xi_q)$. Thus, $N(U_1, \ldots, U_q, c, z) = 0$ has solutions $u_1, \ldots, u_q \in T(\xi_q)$ if and only if z is a norm of an element of $T(\xi_q, \sqrt[q]{c})$ (including the case where the extension $T(\xi_q, \sqrt[q]{c})/T(\xi_q)$ is trivial).

So if we, for example, consider $\mathbf{N}_{L_{\text{inf}}(\sqrt[q]{c})/L_{\text{inf}}}(y) = bx^q + b^q$ with potential solutions y ranging over $L_{\text{inf}}(\sqrt[q]{c})$, then we can conclude that this norm equation is equivalent to a polynomial equation

$$\text{(3.13)} \qquad N(u_1, \ldots, u_q, c, bx^q + b^q) = 0$$

with coefficients in $\mathbb{Z}$ and potential solutions

$$u_1, \ldots, u_q \in L_{\text{inf}} = K_{\text{inf}}(\sqrt[q]{1 + x^{-1}}, \sqrt[q]{1 + (bx^q + b^q)^{-1}}, \sqrt[q]{1 + (c + c^{-1})x^{-1}}).$$

We now would like to replace (3.13) by an equivalent equation but with solutions in

$$L_{2,\text{inf}} = K_{\text{inf}}(\sqrt[q]{1 + x^{-1}}, \sqrt[q]{1 + (bx^q + b^q)^{-1}}).$$

We have to consider two options: either there exists $\gamma \in L_{2,\mathrm{inf}}$ such that

$$\gamma^q = 1 + (c + c^{-1})x^{-1} \tag{3.14}$$

and in this case all the solutions $u_1, \dots, u_q \in L_{2,\mathrm{inf}}$, or $1 + (c + c^{-1})x^{-1}$ is not a q-th power in $L_{2,\mathrm{inf}}$ so that $u_i = \sum_{j=0}^{q-1} u_{i,j}\gamma^j$, where γ is as in (3.14) and $u_{i,j} \in L_{2,\mathrm{inf}}$. In the latter case we can rewrite (3.13) first as

$$N\Bigg(\sum_{j=0}^{q-1} u_{1,j}\gamma^j, \dots, \sum_{j=0}^{q-1} u_{q,j}\gamma^j, c, bx^q + b^q\Bigg) = 0, \tag{3.15}$$

and then as a system of equations over $L_{2,\mathrm{inf}}$ using the fact that the first $q-1$ powers of γ are linearly independent over $L_{2,\mathrm{inf}}$. In other words, we rewrite (3.15) first as

$$\sum_{i=0}^{q-1} N_i(u_{1,0}, \dots, u_{q,q-1}, c, b, x)\gamma^i = 0, \tag{3.16}$$

where N_i are polynomials in listed variables with coefficients in $\mathbb{Z}$, by systematically replacing γ^q via $1 + (c + c^{-1})x^{-1}$ and clearing the denominators (i.e., clearing c from denominators by multiplying through by a sufficiently high power of c), and then as a system

$$\bigwedge_{i=0}^{q-1} N_i(u_{1,0}, \dots, u_{q,q-1}, c, b, x) = 0. \tag{3.17}$$

Note that, even if $\gamma \in L_{2,\mathrm{inf}}$, we can still replace (3.13) by (3.17). To see this reconsider (3.15) as

$$N\Bigg(\sum_{j=0}^{q-1} U_{1,j}\Gamma^j, \dots, \sum_{j=0}^{q-1} U_{q,j}\Gamma^j, C, BX^q + B^q\Bigg) = 0, \tag{3.18}$$

with $U_{i,j}, X, C, B, \Gamma$ algebraically independent over $\tilde{\mathbb{Q}}$, and produce a system of equations

$$\bigwedge_{i=0}^{q-1} N_i(U_{1,0}, \dots, U_{q,q-1}, C, B, X) = 0 \tag{3.19}$$

by the process described above, first systematically replacing Γ^q by

$$1 + (C + C^{-1})X^{-1},$$

clearing the denominators (this time removing C from denominators), and then treating the first $q-1$ powers of Γ as linearly independent over the polynomial ring $\tilde{\mathbb{Q}}[U_{i,j}, X, X^{-1}, C, C^{-1}, B]$. Observe that the left side of (3.18) is equivalent to

$$\sum_{i=0}^{q-1} N_i(U_{1,0}, \ldots, U_{q,q-1}, C, B, X)\Gamma^i$$

modulo the ideal $(\Gamma^q - 1 - (C + C^{-1})X^{-1})$ in the ring

$$\tilde{\mathbb{Q}}[X, X^{-1}, C, C^{-1}, U_{i,j}, B, \Gamma].$$

In other words, for any values of $U_{i,j}, X \neq 0, C \neq 0, B$ in $\tilde{\mathbb{Q}}$ satisfying the system (3.19), we have that (3.18) will be satisfied as long as Γ is set to a value $\gamma \in \tilde{\mathbb{Q}}$ satisfying (3.14), where c and x are the $\tilde{\mathbb{Q}}$-values assigned to C and X respectively. Hence, if (3.17) has solutions $u_{1,0}, \ldots, u_{q,q-1}$ in $L_{2,\mathrm{inf}}$, then (3.13) has solutions $u_0, \ldots, u_{q-1}$ in L_{inf} whether or not the extension $L_{\mathrm{inf}}/L_{2,\mathrm{inf}}$ is trivial.

Conversely, if (3.13) has solutions in $L_{2,\mathrm{inf}}$, we can set $u_{i,0} = u_i$ and $u_{i,j} = 0$ for $j > 0$ and satisfy (3.17) over $L_{2,\mathrm{inf}}$.

Thus for any $c, b, x \in K_{\mathrm{inf}}$ we can conclude that (3.13) has solutions

$$u_1, \ldots, u_q \in L_{\mathrm{inf}}$$

if and only if there exist $u_{1,0}, \ldots, u_{q,q-1} \in L_{2,\mathrm{inf}}$ satisfying (3.15).

Proceeding in the same fashion we can eventually obtain an equivalent system of equations with potential solutions in K_{inf}. Now if a given field H_{inf} does not contain ξ_q or ξ_p, then we can rewrite all the equations one more time so that the final system has solutions and coefficients in H_{inf}. ∎

We can also separate out results concerning integrality at finitely many primes.

THEOREM 3.15: *The following statements are true.*

(1) *If a G-prime $\mathfrak{p}_G$ is completely q-bounded, M is a q-bounding field for $\mathfrak{p}_G$, $b \in K_{\mathrm{inf}}$ is such that for some $\mathfrak{p}_{M(b)} \in \mathscr{C}_{M(b)}(\mathfrak{p}_G)$ we have that $\mathrm{ord}_{\mathfrak{p}_{M(b)}} b \not\equiv 0 \mod q \wedge \mathrm{ord}_{\mathfrak{p}_{M(b)}} b < 0$, and b has no other poles, then the set of all elements $x \in K_{\mathrm{inf}}$ such that $\mathrm{ord}_{\mathfrak{p}_{M(x,b)}} x \geq \frac{q-1}{q} \mathrm{ord}_{\mathfrak{p}_{M(x,b)}} b$ for all $\mathfrak{p}_{M(x,b)} \in \mathscr{C}_{M(b,x)}(\mathfrak{p}_{M(b)})$ is existentially definable. (For future reference in Section 6 denote this set by $\mathrm{Int}(b, \mathfrak{p}_{M(b)}, q)$.)*

(2) *If ramification degrees over G of all factors of $\mathfrak{p}_G$ in number fields contained in I_G are uniformly bounded, then the integral closure of the valuation ring of $\mathfrak{p}_G$ in K_{inf} is existentially definable.*

We now make use of unbounded primes.

THEOREM 3.16: *Let $\mathscr{S}_G \cup \{$ factors of $q\}$ be a completely q-bounded in K_{inf} finite set of primes of G, and let $R_{\text{inf},\mathscr{S}_G}$ be a subring of K_{inf} such that $x \in R_{\text{inf},\mathscr{S}_G}$ if and only if in $G(x)$ the poles of x are either factors of q or primes of $\mathscr{S}_G$, or are at primes that are q-unbounded. In this case $R_{\text{inf},\mathscr{S}_G}$ is first-order definable over K_{inf}.*

Proof. It is enough to consider what happens to the solvability of the norm equation below for c chosen so that factors of q and primes in $\mathscr{S}_G$ split and x has poles only at the primes described in the statement of the theorem. So let $K \in I_G$ and consider

$$\mathbf{N}_{L_K(\sqrt[q]{c})/L_K}(y) = bx^q + b^q. \tag{3.20}$$

As above, since factors of q and primes in $\mathscr{S}_G$ split, this equation will be solvable locally at these primes. Now as far as unbounded primes are concerned, we can always consider the norm equation over a field K large enough so that factors of the unbounded primes occurring with a non-zero order in the divisor of the right side of (3.20) either ramify with ramification degree divisible by q or their relative degree goes up by a factor divisible by q. Over this K, either these factors split completely when we adjoin the q-th root of c or the right side of (3.20) has order divisible by q at the factors of these q-unbounded primes. Thus, in any case of large enough K, the norm equation is solvable at all the factors of unbounded primes. ∎

One can prove a few more variations of such results. The theorem below is another example. Its proof is completely analogous to the proofs above.

THEOREM 3.17: *Let $P = \{p_1, \ldots, p_k\}$ be a finite set of rational primes such that each prime of G not dividing any element of P is herediterily p_i-bounded in K_{inf} with respect to some p_i, and each p_i is completely p_j-bounded in K_{inf} for some p_j. In this case $O_{K_{\text{inf}}}$ is first-order definable over K_{inf}.*

4. Examples of infinite extensions of $\mathbb{Q}$ where the ring of integers is first-order definable

In this section we describe a sample of fields to which our methods apply. Some of these examples will be pretty straightforward while others are more esoteric. We start with the more straightforward examples.

Example 4.1 (Fields with uniformly bounded local degrees): Perhaps the simplest example of a q-bounded infinite extension of rationals is an infinite extension where the local degrees of all primes are uniformly bounded. In such a field every prime is completely q-bounded for any prime q. An example of such an extension is an infinite Galois extension generated by all extensions of degree p (for a fixed prime p) of $\mathbb{Q}$ contained in cyclotomics. More examples of such fields can be found in [1]. Most of such examples where the field is Galois over $\mathbb{Q}$ were already covered by definability results of Videla with respect to the ring of integers. However, one can construct many non-Galois examples of such fields. It is enough to take a collection $\{K_i\}$ of number fields which are Galois but not abelian over $\mathbb{Q}$, linearly disjoint over $\mathbb{Q}$, of degree less than or equal to some fixed n over $\mathbb{Q}$, and consider a collection of number fields $\{N_i\}$, where $N_i \subset K_i$ and N_i is not Galois over $\mathbb{Q}$. Now let N_{inf} be the compositum of all N_i inside $\tilde{\mathbb{Q}}$. If K_{inf} is the compositum of all K_i inside $\tilde{\mathbb{Q}}$, then $N_{\text{inf}} \subset K_{\text{inf}}$ and $[K_{\text{inf}} : N_{\text{inf}}] = \infty$. Thus, while Videla's results give us a first-order definition of $O_{K_{\text{inf}}}$ over K_{inf}, they do not give us a first-order definition of $O_{N_{\text{inf}}}$ over N_{inf}, obtainable by our methods.

Example 4.2 (Galois extensions without cyclic subextensions of degree divisible by arbitrarily high powers of q): If K_{inf} is a Galois extension of a number field G such that for any Galois field $K \in I_G$, we have that $[K : G] \not\equiv 0 \mod q$, then $O_{K_{\text{inf}}}$ and the integral closure of any ring of $\mathscr{S}$-integers in K_{inf} is first-order definable over K_{inf}.

It is not hard to see that in this case ramification and relative degrees in all finite subextensions are prime to q and thus all the primes are completely q-bounded. This example covers cyclotomic extensions with finitely many ramified primes, i.e., extensions of the form $\mathbb{Q}(\xi_{p_1^\ell}, \ldots, \xi_{p_k^\ell}, \ell \in \mathbb{Z}_{>0})$ where $p_1, \ldots, p_k$ are rational primes, and all their subfields that include all abelian extensions with finitely many ramified primes. (The definability of rings of integers in these extensions follows from Videla's results.)

Given a prime q, and an integer $m > 0$, our method also applies to the case of a cyclotomic extension (and any of its subfields) generated by the set

$$\{\xi_{p^\ell} | \ell \in \mathbb{Z}_{>0}, p \neq q \text{ is any prime such that } q^{m+1} \not| (p-1)\}.$$

(In other words we need to omit primes occurring in the arithmetic sequence $kq^{m+1}+1, k \in \mathbb{Z}_{>0}$, and by increasing m we can make the density of the omitted primes arbitrary small.) This example generalizes an example of Fukuzaki where he defined integers over the field $\mathbb{Q}(\{\cos(2\pi/\ell^n) : \ell \in \Delta, n \in \mathbb{Z}_{>0}\})$ and any of its Galois subextensions, and where Δ is the set of all prime integers which are congruent to -1 modulo 4.

On top of such a cyclotomic field we can also add a field generated by any subset of p-th roots of algebraic numbers contained in this cyclotomic field, with p as above not equivalent to 1 modulo q^{m+1}. Clearly, many more examples of Galois extensions of this sort can be generated.

As we pointed out above, being Galois is not required for our method to work. Thus we have some obvious examples of non-Galois extensions where we can define integers.

Example 4.3 (Extensions that are not necessarily Galois): If K_{inf} is a tower of finite extensions of degree less than some positive integer m, then $O_{K_{\text{inf}}}$ and the integral closure of any ring of $\mathscr{S}$-integers in K_{inf} are first-order definable over K_{inf}. Observe that a field of this sort can have primes of arbitrarily large or infinite local degree, and thus this example is a non-trivial generalization of the first example.

If the extension is Galois, we are looking at a field discussed in the second example. So the new cases will come from extensions that are not Galois. Observe that in such a field, for any $q > m$ all the primes are completely q-bounded.

It is more difficult to describe examples where primes are not necessarily completely q-bounded.

Example 4.4 (Less natural fields): Let q be a rational prime and let $\{p_1, \ldots\}$ be a listing of all rational primes omitting q. Let $\pi_i = \prod_{j=1}^{i} p_j$. Let G be any number field and let $\{\mathfrak{p}_1, \ldots\}$ be a listing of all primes of G not lying above q. We construct a tower of fields starting with G where all factors of q are completely q-bounded, all the other primes of G and any finite extension of G are q-bounded but not completely q-bounded and are p-unbounded for any other prime p. Let $K_0 = G$ and assume we have constructed $K_1, \ldots, K_n$ for some $n \geq 0$. We now construct K_{n+1} in three steps.

First we construct an extension $M_{n,1}$ of K_n of degree π_n, where all the primes above $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ will have ramification degrees divisible by π_n and all the primes above q split completely. (Such an extension always exists. For example, take an element a of O_{K_n} such that $\mathrm{ord}_{\mathfrak{p}_i} a = 1$ for $i = 1, \ldots, n$ and $a \equiv 1 \bmod q$ and adjoin $\sqrt[\pi_i]{a}$ to K_n.) This step ensures that the ramification degree of factors of any prime of G not dividing q will eventually be divisible by arbitrarily high powers of rational primes distinct from q.

We now construct a non-trivial extension $M_{n,2}$ of $M_{n,1}$ where all the factors of $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and q in $M_{n,1}$ split completely into distinct factors. (For example, we can adjoin $\sqrt[p]{b}$, where p is prime to $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and q and $b \equiv 1 \mod (q\mathfrak{p}_1 \ldots \mathfrak{p}_n)$.) This step allows us to produce q-bounded and q-unbounded paths above every prime.

Finally K_{n+1} is an extension of $M_{n,2}$ of degree q satisfying the following requirements:

(1) All the factors of q split completely.
(2) For each $i = 1, \ldots, n$ and each $\mathfrak{t}_i$ that is a factor of some $\mathfrak{p}_i$ in $M_{n,1}$, if $\mathfrak{t}_{i,1}, \ldots, \mathfrak{t}_{i,k}$ are factors of $\mathfrak{t}_i$ in $M_{n,2}$ under some ordering, then $\mathfrak{t}_{i,1}$ splits completely into distinct factors and $\mathfrak{t}_{i,2}, \ldots, \mathfrak{t}_{i,k}$ do not split in the extension $K_{n+1}/M_{n,2}$.

To construct such an extension, by Lemma 7.8, we can take a q-th root of an algebraic integer of $M_{n,2}$ such that it is equivalent to $1 \mod q^3$ and modulo $\mathfrak{t}_{i,1}$, and to a non-q-th power modulo $\mathfrak{t}_{i,j}, j \geq 2$. In this step we construct the next level of q-bounded and q-unbounded paths. At the "end" of the construction, every prime of any K_n not dividing q will lie along the "left-most" q-bounded path and the "right-most" q-unbounded path. (In fact, every prime not dividing q will lie along infinitely many q-bounded and q-unbounded paths.)

We now let

$$K_{\mathrm{inf}} = \bigcup_{i=1}^{\infty} K_i.$$

It is easy to see that for all $K \in I_G$ every factor of q is unramified and of relative degree 1. At the same time, for any $p \neq q$, any positive integer m, and any $\mathfrak{p}_i$ prime to q, there is a field $K \in I_G$ where all the factors of $\mathfrak{p}_i$ have a ramification degree over $\mathfrak{p}_i$ divisible by p^m.

Further, for $i \in \mathbb{Z}_{>0}$, let $d_i = \max_{\mathfrak{p}_{K_{i+1}} \in \mathscr{C}_{K_{i+1}}(\mathfrak{p}_i)} \{\mathrm{ord}_q(d(\mathfrak{p}_{K_{i+1}}/\mathfrak{p}_i))\}$, and note that for any $\mathfrak{p}_i$, for any $K \in I_G$ there exists a K-factor $\mathfrak{p}_K$ of $\mathfrak{p}_i$ such that $\mathrm{ord}_q(d(\mathfrak{p}_K/\mathfrak{p}_i)) \leq d_i$, while at the same time for any $m \in \mathbb{Z}_{>0}$, there exist a field $M \in I_G$ and an M-factor $\mathfrak{p}_M$ of $\mathfrak{p}_i$ such that $f(\mathfrak{p}_M/\mathfrak{p}_i) \equiv 0 \mod q^m$.

We can also produce an example where one would need Theorem 3.17. The construction is similar to the one above and, in particular, the existence of extensions we need can be justified by similar arguments.

Example 4.5 (Also not very natural fields): Let $Q = \{q_1, \dots, q_m\}$ be a finite collection of rational primes. Let $\{p_1, \dots\}$ be a listing of all rational primes excluding the primes in Q. Let

$$\pi_i = \prod_{j=1}^{i} p_j.$$

Let G be any number field and divide all the primes of G not lying above any prime of Q into m classes with $\{\mathfrak{p}_{i,j}, i = 1, \dots, m, j \in \mathbb{Z}_{>0}\}$. We now construct a tower of fields $\{K_i\}$ with K_{inf}, as above, being the union of the tower. Let $K_0 = G$ and assume that K_n for some $n \geq 0$ has been constructed. We construct K_{n+1} in $m+1$ steps. First let $M_{0,n}/K_n$ be an extension of degree π_{n+1} such that:

(1) All the primes above primes of Q split completely.
(2) All the primes in the set $\{\mathfrak{p}_{i,j}, i = 1, \dots, m, j = 1, \dots, n+1\}$ ramify completely.

Next we construct $M_{i,n}/M_{i-1,n}$ for $i = 1, \dots, m$. First of all, the degree of the extension will be q_i. Secondly, all the primes above the primes of Q and all the primes above the primes in the set $\{\mathfrak{p}_{i,j}, j = 1, \dots, n+1\}$ split completely. Thirdly, all the primes in the set $\{\mathfrak{p}_{r,j}, r = 1, \dots, m, r \neq i, j = 1, \dots, n+1\}$ remain prime. Finally, $K_{n+1} = M_{m,n}$.

It is not hard to see that for each $i = 1, \dots, m$ the primes $\{\mathfrak{p}_{i,j}, j = 1, \dots, \}$ of G are completely q_i-bounded and these primes are p-unbounded for any prime $p \neq q_i$. Further, all the primes above primes of Q are completely q-bounded for any prime q. Thus we need to use Theorem 3.17 here to get the desired definitions.

We should finish this section with a listing of some obvious fields which are not q-bounded: the algebraic closure of $\mathbb{Q}$, the maximal abelian extension of $\mathbb{Q}$, the field of all totally real numbers, the field of real algebraic numbers. In general, examples of such fields are also not hard to generate. We remind the reader that one would expect the field of all totally real numbers not to be q-bounded since, as has been noted above, the first-order theory of the field of all totally real integers is decidable, while this is not the case for the ring of integers of this field. Thus, the ring of integers of the field of all totally real integers does not have a first-order definition over its fraction field.

5. From undecidability of rings to undecidability of fields

We start with reviewing results we are going to use due to L. Kronecker, J. Robinson and the author of this paper. We first review the results of Julia Robinson from [27].

Theorem 5.1 (JR): *The natural numbers can be defined arithmetically in any totally real algebraic integer ring R such that there is a smallest interval $(0, s)$, s real or ∞, that contains infinitely many sets of conjugates of numbers of R, i.e., infinitely many $x \in R$ with all the conjugates (over $\mathbb{Q}$) in $(0, s)$.*

J. Robinson showed in [27] that certain infinite towers of totally real quadratic extensions have rings of integers with $s = \infty$ and thus the first-order theory of these rings is undecidable. C. Videla used this result in [41] to show that the Pythagorean hull of $\mathbb{Q}$ is undecidable. Further, J. Robinson ([27]), C. Videla ([42]), and K. Fukuzaki ([10]) make use of the following proposition which is a consequence of a result by L. Kronecker from [12].

Proposition 5.2 (Kronecker): *The interval $(0, 4)$ contains infinitely many sets of conjugates of totally real algebraic integers, and no sub-interval of $(0, 4)$ does.*

An immediate consequence of Theorems 5.1 and 5.2 is that in any ring of totally real integers containing a set of the form $\{\cos \frac{2\pi}{m}, m \in \mathscr{X}\}$ with $\mathscr{X}$ an infinite set of positive integers, one can give a first-order definition of integers. Thus, extending results of K. Fukuzaki, we now have the following theorems.

Theorem 5.3: *Let q be a rational prime, let $m > 0$ be an integer and let*

$$K_{\text{inf}} = \mathbb{Q}\left(\cos(2\pi/n), n = \prod_{i=1}^{s} p_i^{\ell_i}, p_i \not\equiv 1 \mod q^m, s, \ell_1, \ldots, \ell_s \in \mathbb{Z}_{>0} \right),$$

where p_i range over all primes satisfying the condition $p \not\equiv 1 \mod q^m$. In this case the first-order theory of K_{inf} is undecidable and $\mathbb{Z}$ is first-order definable in K_{inf}.

Since the ring of all totally real integers is undecidable, every ring of totally real integers is trivially contained in an undecidable ring. However, this is not automatically clear for the fields, since the first-order theory of the field of all totally real numbers is decidable. While we cannot show that the first-order theory of any q-bounded totally real field is undecidable, we can show the following.

Theorem 5.4: *Any q-bounded totally real field is contained in a totally real field that has a first-order definition of rational integers and thus has an undecidable first-order theory.*

Proof. Let $K_{\rm inf}$ be a q-bounded field and observe that $K_{\rm inf}(\cos(2\pi/p^k), k \in \mathbb{Z}_{>0})$ for some $p \neq q$ is also q-bounded, since we will introduce at most a finite number of subextensions of degree divisible by q. (In other words, the increase in divisibility by q of relative or ramification degrees can come only from adding the extension $\mathbb{Q}(\cos 2\pi/p)$ of degree $(p-1)/2$ over $\mathbb{Q}$.) But the ring of integers of the extended field is now undecidable and has a first-order definition of the rational integers, by the discussion above. Thus, since the extended field is still q-bounded, we have that the extended field has a first-order definition of rational integers and an undecidable first-order theory. ∎

We now turn our attention to non-real fields. In [42], C. Videla showed that the ring of integers is definable in infinite Galois extensions of $\mathbb{Q}$ where the degree of every finite subextension is a product of a fixed finite set of primes. Further, as mentioned above, in [43], Videla proved using a theorem of J. Robinson that the ring of integers of $\mathbb{Q}(\xi_{p^r}, r \in \mathbb{Z}_{>0})$ is undecidable. Combining the two results, he also obtained the first-order undecidability of $\mathbb{Q}(\xi_{p^r}, r \in \mathbb{Z}_{>0})$.

Below we prove the following theorem.

Theorem 5.5: *Rational integers are first-order definable in any abelian extension of $\mathbb{Q}$ with finitely many ramified primes, and therefore the first-order theory of such fields is undecidable.*

Rather than relying on the result of J. Robinson, we use existential definability and undecidability results from [35] and [32], where the following result was proven.

Theorem 5.6: *Let $A_{\rm inf}$ be an abelian (possibly infinite) extension of $\mathbb{Q}$ with finitely many ramified primes. Then for any number field $A \subseteq A_{\rm inf}$ and any finite non-empty set $\mathscr{S}_A$ of its primes, we have that $\mathbb{Z}$ is existentially definable in the integral closure of $O_{A,\mathscr{S}_A}$ in $A_{\rm inf}$.*

Now Theorem 5.5 follows from the fact that any abelian extension with finitely many ramified primes must, by L. Kronecker's Theorem, be a subfield of a cyclotomic extension with finitely many ramified primes, i.e., an extension where prime divisors of the degrees of all finite subextensions come from a finite set of primes. Such an extension is q-bounded for any odd q not occurring in the above-mentioned finite set of primes, by Example 4.2. Further, all the primes of $\mathbb{Q}$ are completely q-bounded for such a q. Thus, the integral closure of any ring of $\mathscr{S}$-integers is first-order definable over any abelian extension of $\mathbb{Q}$ with finitely many ramified primes. Therefore by Theorem 5.6 we conclude that rational integers are first-order definable over any abelian extension of $\mathbb{Q}$ with finitely many ramified primes. Since the set of non-zero integers is definable over any ring of algebraic integers, we can "simulate" the field over the ring of integers, and therefore obtain the following corollary:

COROLLARY 5.7: *Rational integers are first-order definable in the ring of integers of any abelian extension of $\mathbb{Q}$ with finitely many ramified primes, and therefore the first-order theory of such a ring is undecidable.*

6. Using elliptic curves with finitely generated groups

In this section we show that over the fields with finitely generated elliptic curves, assuming there exists at least one completely q-bounded prime, we can define $\mathbb{Z}$ and conclude that the first-order theory is undecidable. In [15] it was shown by B. Mazur and K. Rubin that there are large classes of infinite algebraic extensions of $\mathbb{Q}$ satisfying the elliptic curve and a complete q-boundedness condition at the same time.

The use of elliptic curves to investigate definability and decidability has a long history. Perhaps the first mention of elliptic curves in the context of the first-order definability belongs to R. Robinson in [28] and in the context of existential definability to J. Denef in [4]. Using elliptic curves B. Poonen has shown in [19] that if for a number field extension M/K we have an elliptic curve E defined over K, of rank one over K, such that the rank of E over M is also one, then O_K (the ring of integers of K) is Diophantine over O_M. G. Cornelissen, T. Pheidas and K. Zahidi weakened somewhat assumptions of B. Poonen's theorem. Instead of requiring a rank 1 curve retaining its rank in the extension, they require existence of a rank 1 elliptic curve over the bigger field and an abelian variety over the smaller field retaining its positive rank in the extension (see [2]). Further, B. Poonen and the author have independently shown that the conditions of B. Poonen's theorem can be weakened to remove the assumption that the rank is one and require only that the rank in the extension is positive and the same as the rank over the ground field (see [36] and [18]). In [3], G. Cornelissen and the author of this paper used elliptic curves to define a subfield of a number field using one universal and existential quantifiers.

Elliptic curves specifically of rank 1 have been used in several papers in connection to discussions of definability and decidability over big subrings of number fields (i.e., subrings where infinitely many, though not all, primes are inverted). See [20], [23], [7], [17], [8] and [38].

Following J. Denef in [5], as has been mentioned above, the author also considered the situations where elliptic curves had finite rank in infinite extensions and showed that when this happens in a totally real field one can existentially define $\mathbb{Z}$ over the ring of integers of this field and the ring of integers of any extension of degree 2 of such a field (see [37]).

Recently, in [16], B. Mazur and K. Rubin showed that if the Shafarevich–Tate conjecture held over a number field K, then for any prime degree cyclic extension M of K, there existed an elliptic curve of rank one over K, keeping its rank over M. Combined with B. Poonen's theorem, this new result shows that the Shafarevich–Tate conjecture implied HTP is undecidable over the rings of integers of any number field.

C. Videla also used finitely generated elliptic curves to produce undecidability results. His approach, as discussed above, was based on an elaboration by C. W. Henson of a proposition of J. Robinson and results of D. Rohrlich (see [29]) concerning finitely generated elliptic curves in infinite algebraic extensions.

The main ideas for the proof below have been articulated in [3] for the number field case. Here only a minor adjustment is required. We start with reviewing two technical lemmas which can be found in [19]. Let E be an elliptic curve defined over a number field K and fix an affine Weierstrass equation for the curve. Let $P \in E(K)$ be a point of infinite order, let $n \in \mathbb{Z}_{\neq 0}$, and let (x_n, y_n) be the coordinates corresponding to $[n]P$ under the chosen Weierstrass model. Given $x \in K$, let $\mathfrak{n}(x)$ be the integral divisor which is the numerator of the divisor of x in K. Further let $\mathfrak{d}(x) = \mathfrak{n}(x^{-1})$.

LEMMA 6.1: *Let $\mathfrak{A}$ be any integral divisor of K and let m be a positive integer. Then there exists $k \in \mathbb{Z}_{>0}$ such that $\mathfrak{A} | \mathfrak{d}(x_{km})$ in the integral divisor semigroup of K.*

LEMMA 6.2: *There exists a positive integer m such that for any positive integers k, l,*

$$\mathfrak{d}(x_{lm}) | \mathfrak{n}\Big(\frac{x_{lm}}{x_{klm}} - k^2\Big)^2.$$

PROPOSITION 6.3: *Let N/K be a number field extension of degree n. Let $\mathfrak{Q}$ be a prime of K and let $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ be all the primes of N lying above $\mathfrak{Q}$. Let $u \in N$ be integral at $\mathfrak{Q}$. Assume further there exists a sequence $\{(k_i, y_i)\}$ where $k_i \in \mathbb{Z}_{>0}$, $k_{i+1} > k_i$, $y_i \in K$ with $\operatorname{ord}_{\mathfrak{q}_j} y_i \geq 0$ for all i and j, and such that for all i, j we have that $\operatorname{ord}_{\mathfrak{q}_j}(u - y_i) > k_i$. Then $u \in K$.*

Proof. Let $\alpha \in N$ be a generator of N over K such that α is integral with respect to $\mathfrak{Q}$. Let D be the discriminant of the power basis of α. Using this power basis we can represent any $w \in N$ in the following form:

$$w = \sum_{r=0}^{n-1} b_r \alpha^r$$

with $Db_r \in K$ and integral at $\mathfrak{Q}$. Note that for some $a_0, a_1, \ldots, a_{n-1} \in K$ we have that

$$u - y_i = (a_0 - y_i) + \sum_{r=1}^{n-1} a_r \alpha^r$$

and

$$\operatorname{ord}_{\mathfrak{q}_j}(u - y_i) > k_i, \quad j = 1, \ldots, m.$$

Let ℓ be a positive integer and choose i such that $k_i > n(\ell + \operatorname{ord}_{\mathfrak{Q}} D)$. In this case

$$u - y_i \equiv 0 \mod \mathfrak{Q}^{\ell + \operatorname{ord}_{\mathfrak{Q}} D}$$

in the integral closure of the valuation ring of $\mathfrak{Q}$ in N. Let $B \in K$ be such that

$$\operatorname{ord}_{\mathfrak{Q}} B = \ell + \operatorname{ord}_{\mathfrak{Q}} D.$$

Observe that $\frac{u - y_i}{B}$ is integral at $\mathfrak{Q}$, and therefore $D\frac{a_r}{B}$ is integral at $\mathfrak{Q}$ implying that $\operatorname{ord}_{\mathfrak{Q}} a_r \geq \ell$ for $r = 1, \ldots, n-1$. Since ℓ can be arbitrarily large, $a_r = 0$, $r = 1, \ldots, n-1$ and $u \in K$. ∎

We now use our results on defining integrality at a single number field prime to obtain the following theorem.

Theorem 6.4: *Let $\mathfrak{p}_G$ be a prime of G completely q-bounded in K_{inf}. If there exists an elliptic curve E defined over G such that $\operatorname{rank}(E(K_{\text{inf}})) > 0$ and $E(K_{\text{inf}}) = E(G)$, then G is first-order definable over K_{inf} with only one variable in the range of the universal quantifier.*

Proof. Fix an affine Weierstrass equation $y^2 = x^3 + ax + c$ for E and identify non-zero points of $E(K_{\text{inf}})$ with pairs of solutions to the Weierstrass equations as above. Let $b \in K_{\text{inf}}$ be such that it satisfies conditions of Theorem 3.15, Part 1 with respect to all prime factors of $\mathfrak{p}_G$ in $M(b)$, i.e., $\operatorname{ord}_{\mathfrak{p}_{M(b)}} b < 0$ and $\operatorname{ord}_{\mathfrak{p}_{M(b)}} b \not\equiv 0 \mod q$ for all $\mathfrak{p}_{M(b)} \in \mathscr{C}_{M(b)}(\mathfrak{p}_G)$, where M is a completely bounding field for $\mathfrak{p}_G$. Let $u \in K_{\text{inf}}$ be such that $ub \in Int(b, \mathfrak{p}_G, q)$ and

$$\begin{aligned}&\forall z \in K_{\text{inf}} \exists (a_1, b_1),(a_2, b_2) \in E(K_{\text{inf}}) :\\ &\qquad \frac{b^2}{za_1} \in Int(b, \mathfrak{p}_G, q) \wedge (u - \frac{a_1}{a_2})^2 a_1 \in Int(b, \mathfrak{p}_G, q).\end{aligned} \tag{6.1}$$

We claim that if the formula is true for some $u \in N = M(b, u)$, then, by Proposition 6.3, we have that $u \in G$. Indeed, given a $z \in N$ and $\frac{b^2}{za_2} \in Int(b, \mathfrak{p}_G, q)$, we have that for all $\mathfrak{p}_N$ lying above $\mathfrak{p}_G$,

$$\operatorname{ord}_{\mathfrak{p}_N} \frac{b^2}{za_1} > \left(\frac{q-1}{q}\right) \operatorname{ord}_{\mathfrak{p}_N} b$$

implying

$$-\operatorname{ord}_{\mathfrak{p}_N} z + \operatorname{ord}_{\mathfrak{p}_N} \frac{1}{a_1} > \left(\frac{q-1}{q} - 2\right) \operatorname{ord}_{\mathfrak{p}_N} b = \left(-1 - \frac{1}{q}\right) \operatorname{ord}_{\mathfrak{p}_N} b > -\operatorname{ord}_{\mathfrak{p}_N} b > 0.$$

Hence

$$\operatorname{ord}_{\mathfrak{p}_N} \frac{1}{a_1} > \operatorname{ord}_{\mathfrak{p}_N} z - \operatorname{ord}_{\mathfrak{p}_N} b > \operatorname{ord}_{\mathfrak{p}_N} z.$$

The second part of the conjunction in (6.1) now implies

$$\begin{aligned}\operatorname{ord}_{\mathfrak{p}_N} \left(u - \frac{a_1}{a_2}\right)^2 a_1 &> \frac{q-1}{q} \operatorname{ord}_{\mathfrak{p}_N} b,\\ 2 \operatorname{ord}_{\mathfrak{p}_N} \left(u - \frac{a_1}{a_2}\right) &> \frac{q-1}{q} \operatorname{ord}_{\mathfrak{p}_N} b + \operatorname{ord}_{\mathfrak{p}_N} \frac{1}{a_1}\\ &> \frac{q-1}{q} \operatorname{ord}_{\mathfrak{p}_N} b - \operatorname{ord}_{\mathfrak{p}_N} b + \operatorname{ord}_{\mathfrak{p}_N} z > \operatorname{ord}_{\mathfrak{p}_N} z.\end{aligned}$$

Since z can be any element of N and $\frac{a_1}{a_2} \in G$, it follows at once from Proposition 6.3 that $u \in G$.

Now assume that $u = k^2$ with $k \in \mathbb{Z}$. Let $(x_1, y_1) \in E(G)$ be the affine coordinates with respect to a chosen Weierstrass equation of a point $P \in E(G)$ of infinite order, as above. Then by Lemma 6.2 there exists a positive integer m such that for any positive integer l,

$$\mathfrak{d}(x_{lm})|\mathfrak{n}\Big(\frac{x_{lm}}{x_{klm}} - k^2\Big)^2$$

in the integral divisor semigroup of G. Further, by Lemma 6.1 we have that for any positive C, for some r we have that $\mathrm{ord}_{\mathfrak{p}_N} x_{rm} < -C$ for any $\mathfrak{p}_N$. So given a $z \in K_{\mathrm{inf}}$, let $a_1 = x_{rm}, a_2 = x_{krm}$ with r chosen so that $\mathfrak{d}(b^2)\mathfrak{n}(z)|\mathfrak{d}(x_{rm})$ in the integral divisor semigroup of $G(b, z)$, and observe that the first part of the conjunction (6.1) is satisfied. Next we note that for $N = G(b, z)$, since $\mathrm{ord}_{\mathfrak{p}_N} b < 0$, we have that $\mathrm{ord}_{\mathfrak{p}_N} x_{rm} < 0$, and since

$$\mathfrak{d}(x_{rm})|\mathfrak{n}\Big(\frac{x_{rm}}{x_{krm}} - k^2\Big)^2,$$

we also must have that

$$\mathrm{ord}_{\mathfrak{p}_N}\Big(\Big(\frac{x_{rm}}{x_{krm}} - k^2\Big)^2 x_{rm}\Big) \geq 0$$

and thus the second part of the conjunction (6.1) is satisfied.

Finally we note that any positive integer can be written as a sum of four squares, and any element of G can be expressed as a linear combination of some basis elements with rational coefficients. The resulting formula for G is of the form $\exists \dots \exists \forall \exists \dots \exists P$, where P is a polynomial equation. ∎

In view of the theorem above we now have the following.

Theorem 6.5: *Let q be a rational prime and let K_{inf} be an infinite algebraic extension of $\mathbb{Q}$ with at least one prime of a number field contained in K_{inf} completely q-bounded. Assume also there exists an elliptic curve defined over K_{inf} such that its Mordell–Weil group has positive rank and is finitely generated. In this case $\mathbb{Z}$ is first-order definable over this field, and therefore the first-order theory of this field is undecidable.*

This theorem provides another way to improve results due to C. Videla in [43], where finitely generated elliptic curves are used over cyclotomics with one ramified rational prime to generate a model of $\mathbb{Z}$ using results of Julia Robinson. Using these elliptic curves as described above we would also get the first-order definition of $\mathbb{Z}$ as a subset.

Another example of a family of infinite extensions of $\mathbb{Q}$ where one can find finitely generated elliptic curves can be found in [37] where the curves are used to prove existential undecidability of rings of integers. One should note that the fields described in that paper are all q-bounded with respect to almost all rational primes and thus one could also derive the results on the first-order undecidability of these fields using the norm equation method above. In general, the full strength of the elliptic curves method is unknown since we don't have the complete picture concerning elliptic curves in infinite algebraic extensions of $\mathbb{Q}$.

In principle, one can also use Theorem 6.5 to obtain information about existence of finitely generated curves in infinite extensions. If an infinite extension of $\mathbb{Q}$ with a completely q-bounded prime has a decidable first-order theory, then our theorem implies that any elliptic curve defined over the field either has rank 0 or is not finitely generated. Unfortunately (or fortunately), to the best knowledge of the author, we already know, via number-theoretic methods, what the ranks of elliptic curves are over all fields where the first-order theory is known to be decidable.

7. Appendix: Some algebraic number theory

In this section we show how to define a set of elements of a number field containing all integers and such that all non-integers in the set have negative orders (poles) of order divisible by a given prime number q only. We start with some notation.

Notation and Assumptions 7.1: The following notation is used throughout this section. For $x, b, d, a, c \in K \setminus \{0\}$ such that $bx^q + b^q \neq 0, dx^q + d^q \neq 0$, let

$$\begin{aligned}
L_1 =& K(\sqrt[q]{1 + x^{-1}}),\\
L_2 =& L_1(\sqrt[q]{1 + (bx^q + b^q)^{-1}}),\\
L =& L_2(\sqrt[q]{1 + (c + c^{-1})x^{-1}}),\\
F_1 =& K(\sqrt[q]{1 + d^{-1}}),\\
F_2 =& F_1(\sqrt[q]{1 + (dx^q + d^q)^{-1}}),\\
F =& F_2(\sqrt[q]{1 + (a + a^{-1})d^{-1}}),
\end{aligned}$$

and observe that L depends on K, q, x, b, c, while F depends on K, q, a, x, d. For the rest of this section we will assume that x, b, d, a, c take values in K so that all the fields above are defined.

The proof of the lemma below follows from the Hasse–Minkowski Theorem and the fact that over a local field a quaternary form is universal.

Lemma 7.2: *If H is any algebraic extension of $\mathbb{Q}$, then the set*

$$\{x \in H | \exists x_1, x_2, x_3, x_4 \in H : x = x_1^2 + x_2^2 + x_3^2 + x_4^2\}$$

is exactly the set of all elements of H such that for any embedding σ of H into $\tilde{\mathbb{Q}}$ with $\sigma(H) \subset \mathbb{R} \cap \tilde{\mathbb{Q}}$ we have that $\sigma(x) \geq 0$.

Remark 7.3: If K/M is an algebraic extension and $c \in \Omega_2(M)$, then $c \in \Omega_2(K)$. However, $\Omega_2(K) \cap M \neq \Omega_2(M)$ in all cases, since there can be an embedding of K into $\tilde{\mathbb{Q}}$ which is not real but the restriction to the image of M is real. At the same time, if K_{inf} is an infinite algebraic extension of M and $c \in \Omega_2(K_{\text{inf}}) \cap M$, then for some finite extension N of M with $N \subset K_{\text{inf}}$, for all K such that $N \subseteq K \subset K_{\text{inf}}$, we have $c \in \Omega_2(K)$.

Next we state Hensel's lemma and its corollary which play an important role in our use of the Hasse Norm Principle.

Lemma 7.4: *If K is a number field, $f(X) \in K_{\mathfrak{p}_K}[X]$ has coefficients integral at $\mathfrak{p}_K$, and for some $\alpha \in K_{\mathfrak{p}_K}$ integral at $\mathfrak{p}_K$ we have that* $\operatorname{ord}_{\mathfrak{p}_K} f(\alpha) > 2 \operatorname{ord}_{\mathfrak{p}_K} f'(\alpha)$, *then $f(X)$ has a root in $K_{\mathfrak{p}_K}$. (See* [13, Proposition 2, Section 2, Chapter II]*.)*

Corollary 7.5: *If K is a number field, $x \in K$ is integral at all factors of q, $x \equiv 1 \mod q^3$, and $\mathfrak{q}_K$ is any prime of K dividing q, then x is a q-th power in $K_{\mathfrak{q}_K}$.*

Proof. Let $f(X) = X^q - x$ and observe that by our assumption on x we have the following:

$$\operatorname{ord}_{\mathfrak{q}_K} f(1) = \operatorname{ord}_{\mathfrak{q}_K}(1 - x) = 3e(\mathfrak{q}_K/q).$$

At the same time $\operatorname{ord}_{\mathfrak{q}_K} f'(1) = \operatorname{ord}_{\mathfrak{q}_K} q = e(\mathfrak{q}_K/q)$ and therefore

$$\operatorname{ord}_{\mathfrak{q}_K} f(1) > 2 \operatorname{ord}_{\mathfrak{q}_K} f'(1).$$

Hence, by Hensel's lemma $f(x)$ has a root in $K_{\mathfrak{q}_K}$, making x a q-th power. ∎

The two lemmas below, stated without a proof, list some basic number-theoretic facts.

Lemma 7.6: *If F is a number field containing ξ_q, $b \in F$ and b is not a q-th power in F, then the following statements are true:*

1. *If $\operatorname{ord}_{\mathfrak{p}_F} q = \operatorname{ord}_{\mathfrak{p}_F} b = 0$, then $\mathfrak{p}_F$ does not ramify in the extension $F(\sqrt[q]{b})/F$.*
2. *If $\operatorname{ord}_{\mathfrak{p}_F} b = 0$, b is not a q-th power mod $\mathfrak{p}_F$, and $\mathfrak{p}_F$ does not divide q, then $\mathfrak{p}_F$ does not split (i.e., has only one prime above it) in the extension $F(\sqrt[q]{b})/F$.*
3. *If $\operatorname{ord}_{\mathfrak{p}_F} b = 0$, $\mathfrak{p}_F$ does not divide q, and b is a q-th power mod $\mathfrak{p}_F$, then $\mathfrak{p}_F$ splits into distinct factors in the extension $F(\sqrt[q]{b})/F$.*
4. *If $\operatorname{ord}_{\mathfrak{p}_F} b \not\equiv 0 \mod q$, then $\mathfrak{p}_F$ ramifies completely in the extension $F(\sqrt[q]{b})/F$.*

The second lemma deals with norms and primes in cyclic extensions of degree q.

Lemma 7.7: *Let G/F be a cyclic extension of degree q of number fields. If $\mathfrak{p}_F$ is not ramified in the extension, then either it splits completely (in other words, into q distinct factors) or it does not split at all. Further, if $w = \mathbf{N}_{G/F}(z)$ for some $z \in G$, and $\mathfrak{p}_F$ does not split in the extension, then*

$$\operatorname{ord}_{\mathfrak{p}_F} w \equiv 0 \mod q.$$

The following lemma provides a way to avoid ramification of factors of q while taking a q-th root.

Lemma 7.8: *If K is a number field containing ξ_q, a K-prime $\mathfrak{q}_K$ is a factor of q, and*

$$\operatorname{ord}_{\mathfrak{q}_K}(c-1) \geq 3 \operatorname{ord}_{\mathfrak{q}_K} q,$$

then $\mathfrak{q}_K$ splits completely in the extension $K(\sqrt[q]{c})/K$.

Proof. By Corollary 7.5 the polynomial $X^q - c$ has a root in $\mathfrak{q}_K$-adic completion of K, and since the field contains the primitive q-th root of unity, the polynomial has q distinct roots. Thus, the local degree is one for all the factors above $\mathfrak{q}_K$. ∎

The next two propositions explain the purpose of introducing extension

$$L = K(\sqrt[q]{1+x^{-1}}, \sqrt[q]{1+(bx^q+b^q)^{-1}}, \sqrt[q]{1+(c+c^{-1})x^{-1}}).$$

In L:

(1) all primes that are zeros of x and $bx^q + b^q$ ramify unless the order of these zeros is divisible by q;
(2) all primes that are zeros and poles of c ramify unless the order of c at these primes is divisible by q;
(3) we avoid ramifying primes in the cyclic extension obtained by taking the q-th root of c, where we are going to solve norm equations;
(4) we make sure that zeros of x do not have any influence on whether the norm equation has solutions.

Proposition 7.9: *If K is a number field containing ξ_q, and for some elements $b, c \in K$ and some K-prime $\mathfrak{p}_K$ the following assumptions are true:*

(1) $\mathfrak{p}_K$ *is not a factor of* q*,*
(2) c *is not a* q*-th power modulo* $\mathfrak{p}_K$ *(note that this assumption includes the assumption that* $\operatorname{ord}_{\mathfrak{p}_K} c = 0$*),*
(3) $\operatorname{ord}_{\mathfrak{p}_K} x < 0$,
(4) $\operatorname{ord}_{\mathfrak{p}_K} b \not\equiv 0 \mod q$,
(5) $q \operatorname{ord}_{\mathfrak{p}_K} x < (q-1) \operatorname{ord}_{\mathfrak{p}_K} b$,

then for every prime factor $\mathfrak{p}_L$ *of* $\mathfrak{p}_K$ *in* L *we have that*

(1) $\operatorname{ord}_{\mathfrak{p}_L} x < 0$,
(2) c *is not a* q*-th power modulo* $\mathfrak{p}_L$ *and thus not a* q*-th power in* L*, and*
(3) $\operatorname{ord}_{\mathfrak{p}_L} (bx^q + b^q) \not\equiv 0 \mod q$.

Proof. First, by properties of primes and Assumption 3, we have that $\operatorname{ord}_{\mathfrak{p}_L} x < 0$. By Assumption 4, we have that $\operatorname{ord}_{\mathfrak{p}_K} b \not\equiv 0 \mod q$. Next we note that $\operatorname{ord}_{\mathfrak{p}_K}(x^{-1}) > 0$, and therefore by Lemma 7.6, Part 3 we have that $\mathfrak{p}_K$ splits completely into distinct factors in the extension L_1/K. (We remind the reader that $L_1 = K(\sqrt[q]{1 + x^{-1}})$.) Thus, in L_1 we have that $\operatorname{ord}_{\mathfrak{p}_{L_1}} x < 0$, $\operatorname{ord}_{\mathfrak{p}_{L_1}} b \not\equiv 0 \mod q$, and c is not a q-th power modulo $\mathfrak{p}_{L_1}$. We now note that by Assumption 5 we have that $q \operatorname{ord}_{\mathfrak{p}_K} x + \operatorname{ord}_{\mathfrak{p}_K} b < q \operatorname{ord}_{\mathfrak{p}_K} b$, and therefore

$$\operatorname{ord}_{\mathfrak{p}_{L_1}} (bx^q + b^q) = \operatorname{ord}_{\mathfrak{p}_{L_1}} b + q \operatorname{ord}_{\mathfrak{p}_{L_1}} x < 0.$$

Further, by Assumption 4 we have that $\operatorname{ord}_{\mathfrak{p}_{L_1}} (bx^q + b^q) \not\equiv 0 \mod q$. Applying Lemma 7.6, Part 3 again, this time over the field

$$L_2 = L_1(\sqrt[q]{1 + (bx^q + b^q)^{-1}}),$$

we see that in the extension L_2/L_1, the L_1-prime $\mathfrak{p}_{L_1}$ splits completely into distinct factors and thus c is not a q-th power modulo any $\mathfrak{p}_{L_2}$, while

$$\operatorname{ord}_{\mathfrak{p}_{L_2}}(bx^q + b^q) \not\equiv 0 \mod q \quad \text{and} \quad \operatorname{ord}_{\mathfrak{p}_{L_2}}(bx^q + b^q) < 0.$$

Since, by assumption, $\operatorname{ord}_{\mathfrak{p}_K} c = 0$ and therefore $\operatorname{ord}_{\mathfrak{p}_{L_2}} c = 0$, by Lemma 7.6, Part 3 one more time, $\mathfrak{p}_{L_2}$ will split completely into distinct factors in the extension L/L_2 and, as before, this would imply that c is not a q-th power in L or modulo any $\mathfrak{p}_L$ above $\mathfrak{p}_K$. Here we remind the reader that $L = L_2(\sqrt[q]{1+(c+c^{-1})x^{-1}})$. Finally, we also have $\operatorname{ord}_{\mathfrak{p}_L}(bx^q + b^q) \not\equiv 0 \mod q$. ∎

Proposition 7.10: *If K is a number field containing ξ_q, and $x, c, b \in K, L$ are as in Proposition 7.9, then for any L-prime $\mathfrak{a}_L$ that is not a factor of q and is not a pole of x, the following statements hold:*

(1) $\operatorname{ord}_{\mathfrak{a}_L} c \equiv 0 \mod q$;
(2) $\operatorname{ord}_{\mathfrak{a}_L}(bx^q + b^q) \equiv 0 \mod q$;
(3) $\operatorname{ord}_{\mathfrak{a}_L} x \equiv 0 \mod q$.

Proof. We again proceed by applying Lemma 7.6 three times. In the extension L_1/K, where $L_1 = K(\sqrt[q]{1+x^{-1}})$, all the primes that are zeros of x of order not divisible by q are ramified by Lemma 7.6, Part 4, since for any K-prime $\mathfrak{a}_K$ such that $\operatorname{ord}_{\mathfrak{a}_K} x > 0$ we have that $\operatorname{ord}_{\mathfrak{a}_K}(1 + x^{-1}) = \operatorname{ord}_{\mathfrak{a}_K}(x^{-1}) < 0$.

In the extension L_2/L_1, where $L_2 = L_1(\sqrt[q]{1 + (bx^q + b^q)^{-1}})$, as before, we ramify all the primes $\mathfrak{a}_{L_1}$ such that

$$\operatorname{ord}_{\mathfrak{a}_{L_1}}(bx^q + b^q) > 0 \quad \text{and} \quad \operatorname{ord}_{\mathfrak{a}_{L_1}}(bx^q + b^q) \not\equiv 0 \mod q.$$

Further, if $\mathfrak{a}_{L_1}$ is a pole of $bx^q + b^q$ but not a pole of x, then it is a pole of b and therefore $\operatorname{ord}_{\mathfrak{a}_{L_1}}(bx^q + b^q) = q \operatorname{ord}_{\mathfrak{a}_{L_1}} b$.

Finally, $(c + c^{-1})x^{-1}$ has poles at all primes occurring in the divisor of c and not poles of x. Since in L_1, and therefore in L_2, all zeros of x are of order divisible by q, if c has a pole or a zero of degree not divisible by q, and the prime in question is not a pole of x, it follows that $(c + c^{-1})x^{-1}$ has a pole of degree not divisible by q at this prime, forcing it to ramify in the extension $L_2(\sqrt[q]{1 + (c + c^{-1})x^{-1}})/L_2$. Thus, $\operatorname{ord}_{\mathfrak{a}_L} c \equiv 0 \mod q$ for any prime $\mathfrak{a}_L$ not dividing q and not a pole of x. ∎

We now consider what happens to factors of q under cyclic extensions of degree q.

PROPOSITION 7.11: *If for some elements x, d, a of a number field K containing ξ_q and some K-prime $\mathfrak{q}_K$ the following assumptions are true:*

(1) $\mathfrak{q}_K$ *is a factor of* q,
(2) $\mathfrak{q}_K$ *does not split in the extension* $K(\sqrt[q]{a})/K$,
(3) $\operatorname{ord}_{\mathfrak{q}_K} x < 0$,
(4) $\operatorname{ord}_{\mathfrak{q}_K} d \not\equiv 0 \mod q$,
(5) $\operatorname{ord}_{\mathfrak{q}_K} d \le -3 \operatorname{ord}_{\mathfrak{q}_K} q$,
(6) $\operatorname{ord}_{\mathfrak{q}_K} a = 0$,
(7) $q \operatorname{ord}_{\mathfrak{q}_K} x < (q-1) \operatorname{ord}_{\mathfrak{q}_K} d$,

then for every prime factor $\mathfrak{q}_F$ *of* $\mathfrak{q}_K$ *in* F *we have that*

(1) $\operatorname{ord}_{\mathfrak{q}_F} x < 0$,
(2) $\mathfrak{q}_F$ *does not split in the extension* $F(\sqrt[q]{a})/F$, *and*
(3) $\operatorname{ord}_{\mathfrak{q}_F}(dx^q + d^q) \not\equiv 0 \mod q$.

Proof. First of all we note that

$$F = K(\sqrt[q]{1+d^{-1}}, \sqrt[q]{1+(dx^q+d^q)^{-1}}, \sqrt[q]{1+(a+a^{-1})d^{-1}}).$$

Next we observe that over the $\mathfrak{q}_K$-adic completion $K_{\mathfrak{q}_K}$ of K, a q-th root of a generates an unramified extension of degree q. Further, if G/K is a finite extension, where $\mathfrak{q}_K$ has a local degree one (i.e., $e = f = 1$) factor $\mathfrak{q}_G$, then $G_{\mathfrak{q}_G} \cong K_{\mathfrak{q}_K}$, and a q-th root of a generates an unramified extension of degree q over $G_{\mathfrak{q}_G}$, where $\mathfrak{q}_G$ does not split.

Now note that by Assumption 5, we have that $\operatorname{ord}_{\mathfrak{q}_K} d \le -3 \operatorname{ord}_{\mathfrak{q}_K} q$, and therefore by Lemma 7.8 we have that $\mathfrak{q}_K$ splits completely into distinct factors in the extension F_1/K. (We remind the reader that $F_1 = K(\sqrt[q]{1+d^{-1}})$.) Thus, in F_1 we have that $\operatorname{ord}_{\mathfrak{q}_{F_1}} x < 0$, $\operatorname{ord}_{\mathfrak{q}_{F_1}} d \not\equiv 0 \mod q$ and $\mathfrak{q}_{F_1}$ has a factor of relative degree q in the extension generated by adjoining $\sqrt[q]{a}$ to F_1 for any $\mathfrak{q}_{F_1} \in \mathscr{C}_{F_1}(\mathfrak{q}_K)$. Further, by Assumption 7,

$$q \operatorname{ord}_{\mathfrak{q}_K} x + \operatorname{ord}_{\mathfrak{q}_K} d < q \operatorname{ord}_{\mathfrak{q}_K} d \le -3q \operatorname{ord}_{\mathfrak{q}_K} q,$$

and therefore

$$\operatorname{ord}_{\mathfrak{q}_{F_1}}(dx^q + d^q) = \operatorname{ord}_{\mathfrak{q}_{F_1}} d + q \operatorname{ord}_{\mathfrak{q}_{F_1}} x < -3q \operatorname{ord}_{\mathfrak{q}_K} q < 0.$$

Further, by Assumption 4 we have that $\operatorname{ord}_{\mathfrak{q}_{F_1}}(dx^q + d^q) \not\equiv 0 \mod q$. Applying Lemma 7.8 again, this time over the field $F_2 = F_1(\sqrt[q]{1+(dx^q+d^q)^{-1}})$, we see that in the extension F_2/F_1, the F_1-prime $\mathfrak{q}_{F_1}$ splits completely into distinct factors. Consequently, any $\mathfrak{q}_{F_2}$ has a factor of relative degree q in the extension generated by adjoining $\sqrt[q]{a}$ to F_2, while $\operatorname{ord}_{\mathfrak{q}_{F_2}}(dx^q + d^q) \not\equiv 0 \mod q$ and $\operatorname{ord}_{\mathfrak{q}_{F_2}}(dx^q + d^q) < 0$.

Since, by assumption, $\operatorname{ord}_{\mathfrak{q}_K} a = 0$ and therefore $\operatorname{ord}_{\mathfrak{q}_{F_2}} a = 0$, by Lemma 7.8 one more time, $\mathfrak{q}_{F_2}$ will split completely into distinct factors in the extension F/F_2, (here we remind the reader that $F = F_2(\sqrt[q]{1 + (a + a^{-1})d^{-1}})$ and, as before, this would imply that any $\mathfrak{q}_F$ will have a factor of relative degree q in the extension generated by adjoining $\sqrt[q]{a}$ to F, while $\operatorname{ord}_{\mathfrak{q}_F}(dx^q + d^q) \not\equiv 0 \mod q$. So in particular, a is not a q-th power in F. ∎

Now a q-“analog” of Proposition 7.10.

Proposition 7.12: *Under the assumptions of Proposition 7.11, for any F-prime $\mathfrak{a}_F$ that is not a pole of d and is not a pole of x, the following statements hold:*

(1) $\operatorname{ord}_{\mathfrak{a}_F} d \equiv 0 \mod q$;
(2) $\operatorname{ord}_{\mathfrak{a}_F} a \equiv 0 \mod q$;
(3) $\operatorname{ord}_{\mathfrak{a}_F}(dx^q + d^q) \equiv 0 \mod q$.

Proof. We again proceed by applying Lemma 7.6 three times. In the extension F_1/K, where $F_1 = K(\sqrt[q]{1 + d^{-1}})$, all primes that are zeros of d not of order divisible by q are ramified by Lemma 7.6, Part 4, since for any K-prime $\mathfrak{a}_K$ such that $\operatorname{ord}_{\mathfrak{a}_K} d > 0$ we have that $\operatorname{ord}_{\mathfrak{a}_K}(1 + d^{-1}) < 0$.

In the extension F_2/F_1, where $F_2 = F_1(\sqrt[q]{1 + (dx^q + d^q)^{-1}})$, as before, we ramify all the primes $\mathfrak{a}_{F_1}$ such that $\operatorname{ord}_{\mathfrak{a}_{F_1}}(dx^q+d^q) > 0$ and $\operatorname{ord}_{\mathfrak{a}_{F_1}}(dx^q+d^q) \not\equiv 0 \mod q$. Further, if $\mathfrak{a}_K$ is a pole of $dx^q + d^q$ but $\mathfrak{a}_K$ is not a pole of d, then $\operatorname{ord}_{\mathfrak{a}_K}(dx^q+d^q) = q \operatorname{ord}_{\mathfrak{a}_K} x$, and if for some pole $\mathfrak{q}_K$ of d we have that $\operatorname{ord}_{\mathfrak{q}_K} x > 0$, then

$$\operatorname{ord}_{\mathfrak{q}_K}(dx^q + d^q) = q \operatorname{ord}_{\mathfrak{q}_K} d.$$

Finally, $(a + a^{-1})d^{-1}$ has poles at all primes occurring in the divisor of a and not poles of d. Further, in F_2 all zeros of d are of orders divisible by q. Thus if a has a pole or a zero of degree not divisible by q, it follows that $(a + a^{-1})d^{-1}$ has a pole of degree not divisible by q at this prime, forcing it to ramify in the extension $F_2(\sqrt[q]{1 + (a + a^{-1})d^{-1}})/F_2$. Thus, $\operatorname{ord}_{\mathfrak{a}_F} a \equiv 0 \mod q$ for any prime $\mathfrak{a}_F$ as described in the statement of the proposition. ∎

The lemma below considers some archimedean completions of a number field.

LEMMA 7.13: *If $c \in \Omega_2(K)$ and $M = K(\sqrt{c})$, then any archimedean completion of M is isomorphic to the corresponding archimedean completion of K.*

Proof. Let σ be an embedding of M into $\tilde{\mathbb{Q}}$. If $\sigma(M) \subset \tilde{\mathbb{Q}} \cap \mathbb{R}$, then the archimedean completion of $\sigma(M)$ is isomorphic to $\mathbb{R}$, and the completion is isomorphic to $\mathbb{C}$ otherwise. Therefore to prove the lemma, it is enough to show that whenever $\sigma(K) \subset \tilde{\mathbb{Q}} \cap \mathbb{R}$, we also have $\sigma(M) \subset \tilde{\mathbb{Q}} \cap \mathbb{R}$. This implication follows from the fact that whenever $\sigma(K) \subset \tilde{\mathbb{Q}} \cap \mathbb{R}$, we have $\sigma(c) > 0$ and therefore $\sqrt{\sigma(c)} \in \mathbb{R}$. ∎

We will need the two lemmas below when analyzing what happens to factors of q in number field extensions of degree q.

LEMMA 7.14: *If U/K is a Galois extension of number fields, F/U is a cyclic number field extension, and the extension F/K is Galois, then there are infinitely many primes of U not splitting in the extension F/U and lying above a prime of K splitting completely in U.*

Proof. If σ is a generator of $\mathrm{Gal}(F/U)$, then any prime of F whose Frobenius over K is

$$\sigma \in \mathrm{Gal}(F/U) \subset \mathrm{Gal}(F/K)$$

will have the desired property. Now the Tchebotarev Density Theorem tells us that there are infinitely many such primes. ∎

LEMMA 7.15: *Let F/U be a cyclic extension of number fields such that for some rational prime q we have that $[F : U] \equiv 0 \mod q^m$. Let N be the unique subfield of F containing U such that $[N : U] = q^m$. Let $\mathfrak{p}_F$ be a prime of F and let $\mathfrak{p}_U$ be the U-prime below it. If σ is the Frobenius automorphism of $\mathfrak{p}_F$ and σ is not a q-th power in Gal(F/U), then $\mathfrak{p}_U$ does not split in the extension N/U.*

Proof. Observe that $\mathrm{Gal}(F/N)$ is the set of all elements of the Galois group that are q^m-th powers. Thus, since σ is not a q-th power in $\mathrm{Gal}(F/U)$, we must have that q^m is the smallest positive power r of σ such that $\sigma^r \in \mathrm{Gal}(F/N)$. Therefore, we have that $\sigma_{|N}$ has order q^m and thus generates the Galois group of N over U. Hence, the decomposition group of $\mathfrak{p}_F \cap N = \mathfrak{p}_N$ is the Galois group of N/U, and $\mathfrak{p}_U$ does not split in the extension N/U. ∎

We now construct a cyclic extension of degree equal to a power of q, where q can have an arbitrarily high relative degree and no ramified factors.

Lemma 7.16: *If q is a rational prime, $m \in \mathbb{Z}_{>0}$, then there exists a totally real cyclic extension of $\mathbb{Q}$ of degree q^m where q does not split.*

Proof. Let ℓ be a rational prime satisfying the following conditions:

(1) ℓ splits completely in $\mathbb{Q}(\xi_{q^m})/\mathbb{Q}$.

(2) Factors of ℓ in $\mathbb{Q}(\xi_{q^m})$ do not split in the extension $\mathbb{Q}(\xi_{q^m}, \sqrt[q]{q})/\mathbb{Q}(\xi_{q^m})$.

(Observe that by Lemma 7.14 there are infinitely many such ℓ's.) It follows that $\ell \equiv 1 \mod q^m$, but q is not a q-th power mod ℓ. Indeed, since both bases $\{1, \xi_q, \dots, \xi_q^{(q-1)q^{m-1}}\}$ and $\{1, \sqrt[q]{q}, \dots, \sqrt[q]{q^{q-1}}\}$ are integral bases with respect to ℓ and all of its factors, the factorization of ℓ and its factors in the extensions $\mathbb{Q}(\xi_{q^m})/\mathbb{Q}$ and $\mathbb{Q}(\xi_{q^m}, \sqrt[q]{q})/\mathbb{Q}(\xi_q)$ corresponds to the factorization of the respective minimal polynomials modulo ℓ. Consequently, $\mathbb{Z}/\ell$ contains a q^m-th root of unity, so that $q^m|(\ell-1)$, and the polynomial $T^q - q$ has no roots modulo any factors ℓ in $\mathbb{Q}(\xi_q)$.

Now consider the extension $\mathbb{Q}(\xi_\ell)/\mathbb{Q}$ and note that it is of degree divisible by q^m. If τ is the Frobenius of q, then $\tau(\xi_\ell) = \xi_\ell^q$ and τ is not a q-th power in $\mathrm{Gal}(\mathbb{Q}(\xi_\ell)/\mathbb{Q})$. Indeed, suppose $\tau = \sigma^q$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_\ell)/\mathbb{Q})$. Let r be a positive integer such that $\sigma(\xi_\ell) = \xi_\ell^r$ and therefore

$$\xi_\ell^q = \tau(\xi_\ell) = \sigma^q(\xi_\ell) = \xi_\ell^{r^q},$$

implying $q \equiv r^q \mod \ell$ in contradiction to our assumption on ℓ and q. Therefore, by Lemma 7.15, we conclude that q will not split in the unique degree q^m extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\xi_\ell)$. ■

We now use the lemma above to construct a cyclic extension of a number field where q has relative degree q and no ramified factors. We do this in two steps. The first step is the lemma below.

Lemma 7.17: *If G is algebraic over $\mathbb{Q}$, H a number field with $H/\mathbb{Q}$ cyclic, then GH/G is cyclic with $[GH : G]|[H : \mathbb{Q}]$.*

Proof. If $A = G \cap H$, then, since $H/\mathbb{Q}$ is Galois, $[H : A] = [GH : G]$ and thus $[GH : G]$ divides $[H : \mathbb{Q}]$. Indeed, let $\alpha \in H$ generate H over $\mathbb{Q}$ and therefore also GH over G, and let $a_0 + a_1T + \cdots + T^r$ be the monic irreducible polynomial of α over G. Since all the conjugates of α over $\mathbb{Q}$ are in H, all the conjugates of α over G are in H, and thus $a_0, \ldots, a_{r-1} \in H$ and hence in A. So the degree of α over G is at least as large as the degree of α over A. Since $A \subseteq G$, these degrees must be equal.

Further, H/A is again a cyclic extension, and all the conjugates of α over A and over G are the same. Hence,

$$\mathrm{Gal}(GH/G) \cong \mathrm{Gal}(H/A)$$

and we can conclude that the extension GH/G is cyclic. ∎

This is the second step of our construction.

Lemma 7.18: *Let G be a number field such that for some prime $\mathfrak{p}_G$ of G lying above a rational prime $\mathfrak{p}_{\mathbb{Q}}$ we have that $\mathrm{ord}_q(f(\mathfrak{p}_G/\mathfrak{p}_{\mathbb{Q}})) = m$. Suppose now that H is a cyclic extension of $\mathbb{Q}$ of degree q^r with $r > m$, where $\mathfrak{p}_{\mathbb{Q}}$ does not split. Let GH be the field compositum of G and H inside the chosen algebraic closure of $\mathbb{Q}$. Under these assumptions, there exists a field $\hat{G}$ such that $G \subseteq \hat{G} \subset GH$ and $GH/\hat{G}$ is a cyclic extension of degree q where no factor of $\mathfrak{p}_H$ splits.*

Proof. Consider the following field diagram:

$$\begin{tikzcd}
\mathfrak{p}_{GH} \in GH & \mathfrak{p}_G \in G \arrow[l] \\
\mathfrak{p}_H \in H \arrow[u] & \mathfrak{p}_{\mathbb{Q}} \in \mathbb{Q} \arrow[l] \arrow[u]
\end{tikzcd}$$

and observe that $f(\mathfrak{p}_{GH}/\mathfrak{p}_{\mathbb{Q}}) \geq q^r$, while $\mathrm{ord}_q(f(\mathfrak{p}_G/\mathfrak{p}_{\mathbb{Q}})) = m < r$. Consequently,

$$\mathrm{ord}_q(f(\mathfrak{p}_{GH}/\mathfrak{p}_G)) > 1$$

and thus $f(\mathfrak{p}_{GH}/\mathfrak{p}_G) > 1$. By Lemma 7.17, the extension GH/G is cyclic of degree that is a power of q. Further, by Proposition 8, of Chapter II, §4 of [13], GH/G is unramified at all the factors of $\mathfrak{p}_G$. Let σ be a generator of the $\mathrm{Gal}(GH/G)$ and observe that for some positive integer i, the Frobenius automorphism of any factor $\mathfrak{p}_{GH}$ of $\mathfrak{p}_G$ over G is $\sigma^i \neq \mathrm{id}$ and must be of order divisible by q. Now, if $\hat{G} \neq GH$ is the fixed field of $\sigma^{\mathrm{ord}\,\sigma^i/q}$, we have that any factor $\mathfrak{p}_{\hat{G}}$ of $\mathfrak{p}_G$ in $\hat{G}$ will not split in the extension $GH/\hat{G}$ and $[GH : \hat{G}] = q$. ∎

Since for any G and H as above, the field $\hat{G}$ satisfying $G \subset \hat{G} \subset GH$ and $[GH : \hat{G}] = q$ is unique, we have the following corollary.

Corollary 7.19: *Let G, H be as in Lemma 7.18, and assume additionally that for any G-prime $\mathfrak{p}_G$ lying above a rational prime $\mathfrak{p}_{\mathbb{Q}}$ we have that*

$$\operatorname{ord}_q f(\mathfrak{p}_G/\mathfrak{p}_{\mathbb{Q}}) < [H : \mathbb{Q}].$$

Let $\hat{G}$ be a subfield of GH such that $G \subset \hat{G}$ and $[GH : \hat{G}] = q$. In this case no $\hat{G}$-factor of $\mathfrak{p}_{\mathbb{Q}}$ splits in the extension $GH/\hat{G}$.

We now consider the case when $q = 2$ and examine generators of GH over $\hat{G}$.

Lemma 7.20: *Let $G, \hat{G}, H$ be as in Corollary 7.19, let $q = 2$, and assume H is totally real. Suppose $HG = \hat{G}(\sqrt{a})$, $a \in \hat{G}$. In this case, if $\sigma : \hat{G} \longrightarrow \tilde{\mathbb{Q}} \cap \mathbb{R}$ is an embedding of $\hat{G}$, then $\sigma(a) > 0$.*

Proof. Since H is totally real, for any embedding $\sigma : HG \longrightarrow \tilde{\mathbb{Q}}$, we have that

$$\sigma(HG) \subset \mathbb{R} \Leftrightarrow \sigma(G) \subset \mathbb{R}.$$

If $\sigma(\hat{G}) \subset \mathbb{R}$, then $\sigma(G) \subset \mathbb{R}$ and $\sigma(HG) \subset \mathbb{R}$ implying $\sqrt{\sigma(a)} \in \mathbb{R}$ and $\sigma(a) \geq 0$. ∎

References

[1] S. Checcoli, *Fields of algebraic numbers with bounded local degrees and their properties*, Transactions of the American Mathematical Society **365** (2013), 2223–2240.

[2] G. Cornelissen, T. Pheidas and K. Zahidi, *Division-ample sets and diophantine problem for rings of integers*, Journal de Théorie des Nombres Bordeaux **17** (2005), 727–735.

[3] G. Cornelissen and A. Shlapentokh, *Defining the integers in large rings of number fields using one universal quantifier*, Rossiĭskaya Akademiya Nauk. Sankt-Peterburgskoe Otdelenie. Matematicheskiĭ Institut imeni V. A. Steklova. Zapiski Nauchnykh Seminarov (POMI) **358** (2008), 199–223.

[4] J. Denef, *Diophantine sets of algebraic integers, II*, Transactions of the American Mathematical Society **257** (1980), 227–236.

[5] J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers*, Journal of the London Mathematical Society **18** (1978), 385–391.

[6] J. Denef, L. Lipshitz, T. Pheidas and J. Van Geel (eds.), *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, volume 270 of Contemporary Mathematics, Vol. 270, American Mathematical Society, Providence, RI, 2000.

[7] K. Eisenträger and G. Everest, *Descent on elliptic curves and Hilbert's tenth problem*, Proceedings of the American Mathematical Society **137** (2009), 1951–1959.

[8] K. Eisenträger, G. Everest and A. Shlapentokh, *Hilbert's tenth problem and Mazur's conjectures in complementary subrings of number fields*, Mathematical Research Letters **18** (2011), 1141–1162.

[9] M. D. Fried, D. Haran and H. Völklein, *Real Hilbertianity and the field of totally real numbers*, in *Arithmetic Geometry (Tempe, AZ, 1993)*, Contemporary Mathematics, Vol. 174, American Mathematical Society, Providence, RI, 1994, pp. 1–34.

[10] K. Fukuzaki, *Definability of the ring of integers in some infinite algebraic extensions of the rationals*, MLQ Mathematical Logic Quarterly **58** (2012), 317–332.

[11] J. Koenigsmann, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, Annals of Mathematics **183** (2016), 79–93.

[12] L. Kronecker, *Zwei sätze über gleichungen mit ganzzahligen coefficienten*, Journal für die Reine und Angewandte Mathematik **53** (1857), 173–175.

[13] S. Lang, *Algebraic Number Theory*, Addison Wesley, Reading, MA, 1970.

[14] S. Lang, *Algebra*, Graduate Texts in Mathematics, Vol. 211, Springer-Verlag, New York, 2002.

[15] B. Mazur and K. Rubin, *Diophantine stability*, arXiv:1503.04642.

[16] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's Tenth Problem*, Inventiones Mathematicae **181** (2010), 541–575.

[17] S. Perlega, *Additional results to a theorem of Eisenträger and Everest*, Archiv der Mathematik **97** (2011), 141–149.

[18] B. Poonen, *Elliptic curves whose rank does not grow and Hilbert's Tenth Problem over the rings of integers*, Private Communication.

[19] B. Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's Tenth Problem over rings of algebraic integers*, in *Algorithmic Number Theory (Sidney, 2002)*, Lecture Notes in Computer Science, Vol. 2369, Springer, Berlin, 2002, pp. 33–42.

[20] B. Poonen, *Hilbert's Tenth Problem and Mazur's conjecture for large subrings of $\mathbb{Q}$*, Journal of the American Mathematical Society **16** (2003), 981–990.

[21] B. Poonen, *Undecidability in number theory*, Notices of the American Mathematical Society **55** (2008), 344–350.

[22] B. Poonen, *Characterizing integers among rational numbers with a universal-existential formula*, American Journal of Mathematics **131** (2009), 675–682.

[23] B. Poonen and A. Shlapentokh, *Diophantine definability of infinite discrete nonarchimedean sets and diophantine models for large subrings of number fields*, Journal für die Reine und Angewandte Mathematik **588** (2005), 27–48.

[24] I. Reiner, *Maximal Orders*, London Mathematical Society Monographs. Vol. 28, The Clarendon Press, Oxford University Press, Oxford, 2003.

[25] J. Robinson, *Definability and decision problems in arithmetic*, Journal of Symbolic Logic **14** (1949), 98–114.

[26] J. Robinson, *The undecidability of algebraic fields and rings*, Proceedings of the American Mathematical Society **10** (1959), 950–957.

[27] J. Robinson, *On the decision problem for algebraic rings*, in *Studies in Mathematical Analysis and Related Topics*, Stanford University Press, Stanford, CA, 1962, pp. 297–304.

[28] R. M. Robinson, *The undecidability of pure transcendental extensions of real fields*, Zeitschrift für Mathematische Logik und Grundlagen der Mathematik **10** (1964), 275–282.

[29] D. E. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Inventiones Mathematicae **75** (1984), 409–423.

[30] R. Rumely, *Undecidability and definability for the theory of global fields*, Transactions of the American Mathematical Society **262** (1980), 195–217.

[31] R. S. Rumely, *Arithmetic over the ring of all algebraic integers*, Journal für die Reine und Angewandte Mathematik **368** (1986), 127–133.

[32] A. Shlapentokh, *Diophantine undecidability in some rings of algebraic numbers of totally real infinite extensions of* $\mathbb{Q}$, Annals of Pure and Applied Logic **68** (1994), 299–325.

[33] A. Shlapentokh, *First-order definitions of rational functions and* $\mathscr{S}$*-integers over holomorphy rings of algebraic functions of characteristic* 0, Annals of Pure and Applied Logic **136** (2005), 267–283.

[34] A. Shlapentokh, *Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields*, New Mathematical Monographs, Vol. 7, Cambridge University Press, Cambridge, 2006.

[35] A. Shlapentokh, *Diophantine definability and decidability in the extensions of degree 2 of totally real fields*, Journal of Algebra **313** (2007), 846–896.

[36] A. Shlapentokh, *Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers*, Transactions of the American Mathematical Society **360** (2008), 3541–3555.

[37] A. Shlapentokh, *Rings of algebraic numbers in infinite extensions of* $\mathbb{Q}$ *and elliptic curves retaining their rank*, Archive for Mathematical Logic **48** (2009), 77–114.

[38] A. Shlapentokh, *Elliptic curve points and Diophantine models of* $\mathbb{Z}$ *in large subrings of number fields*, International Journal of Number Theory **8** (2012), 1335–1365.

[39] A. Tarski, *A decision method for elementary algebra and geometry*, in *Collected Papers. Vol. 3: 1945–1957*, Contemporary Mathematicians, Birkhäuser, Basel, 1986.

[40] L. van den Dries, *Elimination theory for the ring of algebraic integers*, Journal für die Reine und Angewandte Mathematik **388** (1988), 189–205.

[41] C. Videla, *On the constructible numbers*, Proceedings of the American Mathematical Society **127** (1999), 851–860.

[42] C. Videla, *Definability of the ring of integers in pro-p extensions of number fields*, Israel Journal of Mathematics **118** (2000), 1–14.

[43] C. R. Videla, *The undecidability of cyclotomic towers*, Proceedings of the American Mathematical Society **128** (2000), 3671–3674.

[44] A. Weil, *Basic Number Theory*, Die Grundlehren der Mathematischen Wissenschaften, Vol. 144, Springer Verlag, New York–Berlin, 1974.